



Kolodynski, J., Máttar, A., Skrzypczyk, P., Woodhead, E., Cavalcanti, D., Banaszek, K., & Acín, A. (2020). Device-independent quantum key distribution with single-photon sources. *Quantum*, 4, [260 (2020)].
<https://doi.org/10.22331/q-2020-04-30-260>

Publisher's PDF, also known as Version of record

License (if available):
CC BY

Link to published version (if available):
[10.22331/q-2020-04-30-260](https://doi.org/10.22331/q-2020-04-30-260)

[Link to publication record in Explore Bristol Research](#)
PDF-document

This is the final published version of the article (version of record). It first appeared online via Quantum at <https://quantum-journal.org/papers/q-2020-04-30-260/>. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available:
<http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/>

Device-independent quantum key distribution with single-photon sources

J. Kołodyński^{1,2}, A. Máttar², P. Skrzypczyk³, E. Woodhead^{2,4}, D. Cavalcanti², K. Banaszek^{1,5}, and A. Acín^{2,6}

¹Centre for Quantum Optical Technologies, Centre of New Technologies, University of Warsaw, Banacha 2c, 02-097 Warsaw, Poland

²ICFO-Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

³H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom

⁴Laboratoire d'Information Quantique, Université libre de Bruxelles (ULB), 1050 Bruxelles, Belgium

⁵Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warszawa, Poland

⁶ICREA-Institució Catalana de Recerca i Estudis Avançats, Lluís Companys 23, 08010 Barcelona, Spain

Device-independent quantum key distribution protocols allow two honest users to establish a secret key with minimal levels of trust on the provider, as security is proven without any assumption on the inner working of the devices used for the distribution. Unfortunately, the implementation of these protocols is challenging, as it requires the observation of a large Bell-inequality violation between the two distant users. Here, we introduce novel photonic protocols for device-independent quantum key distribution exploiting *single-photon sources* and *heralding-type architectures*. The heralding process is designed so that transmission losses become irrelevant for security. We then show how the use of single-photon sources for entanglement distribution in these architectures, instead of standard entangled-pair generation schemes, provides significant improvements on the attainable key rates and distances over previous proposals. Given the current progress in single-photon sources, our work opens up a promising avenue for device-independent quantum key distribution implementations.

1 Introduction

The paradigm of *device-independent quantum key distribution* (DIQKD) offers the strongest form of secure communication, relying only on the validity of quantum mechanics, but not on any detailed description, or trust, of the inner workings of the users' devices [1–3]. On the theoretical side, the security of DIQKD has been proven against increasingly powerful eavesdroppers [4, 5], culminating in proofs of security against attacks of the most general form [6, 7].

The main challenge facing experimental DIQKD are its stringent demands on the observable data, necessary for the security requirements to be met. First, any DIQKD implementation should be based

on the observation of data that conclusively violates a Bell inequality [8, 9]. In particular, the Bell experiment should close the so-called *detection loophole* [10], otherwise, hacking attacks can fake a violation at the level of the detected events when losses are high enough [11]. Moreover, a detection-loophole-free Bell violation is necessary but not sufficient for secure DIQKD, as the necessary detection efficiencies are significantly higher than those required for Bell violation. For instance, while the detection efficiency for observing a Bell violation of the Clauser-Horne-Shimony-Holt (CHSH) [12] inequality can be as low as $2/3$ [13], a DIQKD protocol based on CHSH requires an efficiency of the order of 90% [3]. This is, in fact, a general feature of any noise parameter—consider, e.g. the visibility [4]—that affects not only the observed Bell violation, but also the correlations between the users aiming to construct the secret key.

The first Bell experiments closing the detection loophole used massive particles [14–17]. Leaving aside table-top [14, 15] and short-distance [16] experiments, the Bell test of Hensen et al. [17] involved labs separated by a distance of 1.3 km, which allowed to close also the *locality loophole* [9]. Nevertheless, as the employed light-matter interaction processes typically deteriorate the quality of the nonlocal correlations generated between the users, the reported violations would not have been sufficient for secure DIQKD. Furthermore, the rates of key distribution they could provide are seriously limited owing to the measurements involved that, despite allowing for near unit efficiency, take significant time [18, 19]. While improvements are to be expected in all these issues, and massive particles may be essential for long-distance schemes involving quantum repeaters [20], photon-based schemes appear more suitable to obtain high key rates with current or near-future technology. Photonic losses, however, occurring at all of the generation, transmission, and detection stages represent the main challenge in these schemes. Recent advances have been made for photo-detection efficien-

cies, which allowed for the first loophole-free photonic Bell inequality violations over short distances [21–24]. Still, not only are the reported distances far from any cryptographic use, but also the observed Bell violations are again not large enough for secure DIQKD.

In this work, we show that *single-photon sources* [25] constitute a promising resource for experimental photonic DIQKD. Such sources have already allowed for nearly on-demand [26], highly efficient [27] extraction of single photons (also in pulse trains [28, 29] as well as at telecom wavelengths [30]), while maintaining their purity and indistinguishability even above the 99% level [31, 32]. We propose novel DIQKD photonic schemes that thanks to the replacement of the photon-pair creation process (achieved, e.g. by parametric downconversion [33]) with single-photon sources allow to distribute the key at significant rates over large distances. We believe that, in view of the recent advances in the fabrication of single-photon sources, our results point out a promising avenue for DIQKD implementations.

The remainder of the paper is organized as follows. In Sec. 2.2, we describe the technique of evading transmission losses in DIQKD protocols by means of heralding and, furthermore, discuss the crucial implications the heralding method has for designing photon-based architectures. Subsequently, in Sec. 3, we introduce two heralded schemes employing single-photon sources, which allow for fine-tuning of the final shared entangled state, important for achieving optimal efficiencies. We then discuss in Sec. 4 how to quantify the attainable key rates within a heralded scheme, which importantly are then guaranteed to be fully secure. Finally, in Sec. 5 we apply our analysis to the two schemes proposed, in order to study their performance, in particular, the key rates, separation distances, as well as noise levels they allow for in DIQKD. We conclude our work in Sec. 6.

2 Losses in DIQKD

For non-negligible key rates to be achievable over large distances in DIQKD, solutions must be proposed that pinpoint and disregard—without opening the detection loophole—inconclusive protocol rounds that arise due to photons being inevitably lost. From the perspective of maintaining security (i.e. only the question of non-zero key rate), it is convenient then to divide photonic losses into two categories. Losses that occur within the *local* surroundings—laboratories—of the users should be differentiated from those that occur during the *transmission* of photons between the labs. Laboratories represent then regions of space from, and into which, the users control the information flow, i.e. provide the local privacy requisite for any secure communication [34].

As a result, one may design DIQKD protocols that target explicitly the transmission losses and allow for

Bell violations over arbitrary distances between the users [35, 36]. Other approaches have also been proposed that, while stemming from novel entropic uncertainty relations which account for quantum side information [37, 38], require only local Bell violation within one of the labs [39]. This, however, comes at the price of security being guaranteed only up to a finite distance separating the users for a given fixed, even arbitrarily small, level of local losses (also in the absence of detector dark-count events [40]). In this work, our goal is to propose optical schemes where the security can be guaranteed independently of the distance between the users. Secondary to this, for a scheme to be practical, we furthermore want the resulting key rate to scale favourably with the separation, in order to achieve non-negligible key rates over large distances.

2.1 Local losses

We parametrise local losses by the effective *local efficiency*, η , which accounts for all photon-loss mechanisms inside the lab, including imperfect photo-detection, any optical path and mode mismatch, finite photon-extraction efficiency of the sources locally employed by a user, etc. To our knowledge, all known DIQKD protocols require a high local efficiency, of the order of 90% [36, 39, 41–44]. While the existence of practical DIQKD protocols tolerating lower local efficiencies cannot be excluded, we do not expect any significant improvement in this direction. This is a consequence of the following simple argument.

A generic DIQKD protocol is based upon the observation of some ideal correlations described by a set of joint probability distributions $\mathbf{p} = \{P(ab|xy)\}_{abxy}$ shared by the two users, Alice and Bob, that aim to establish the secret key. The input random variable, x (y), labels the measurement setting, i.e. the measurement that Alice (Bob) has chosen, while the output, a (b), stands for the outcome of her (his) measurement. In the presence of local losses, parametrised by η , there is an additional outcome, labelled by ϕ , corresponding to the ‘no-detection’ event. The resulting correlations observed, \mathbf{p}^η , where a and b refer only to ‘conclusive’ events, are

$$\begin{aligned} P^\eta(ab|xy) &= \eta^2 P(ab|xy) \\ P^\eta(a\phi|xy) &= \eta P_A(a|x) (1 - \eta) \\ P^\eta(\phi b|xy) &= (1 - \eta) \eta P_B(b|y) \\ P^\eta(\phi\phi|xy) &= (1 - \eta)^2, \end{aligned} \quad (1)$$

where P_A and P_B denote the marginal probabilities detected by Alice and Bob in the ideal case (without loss). For simplicity, we take the local efficiencies equal for Alice and Bob and for all measurement settings, but the results can be easily generalized to non-equal local efficiencies.

In any DIQKD protocol, Alice and Bob construct the key from the outputs of n_k pairs of measurement

settings (typically $n_k = 1$, and the key is generated from the pair (x^*, y^*) [36, 41–44]). In Ref. [45], a successful eavesdropping attack was constructed for a critical value of the losses equal to $\eta_c = 1/(n_k + 1)$ if $n_k < m$, where m is the total number of measurement settings, and $\eta_c = 1/m$ when $n_k = m$. To implement this attack, Eve needs to be able to control the detection efficiencies on one side, say Alice. Eve has perfect knowledge of the outputs of the n_k measurements used by Alice for the key, while reproducing the expected correlations (1) for $\eta_l = \eta_c$.

For detection efficiencies above this critical value, $\eta_l > \eta_c$, Eve can use a combined strategy, in which the previous attack is applied on Alice’s side with probability q_A , while with probability $1 - q_A$ Eve does nothing on the measured state and shifts Alice’s detection efficiency to one. This attack produces correlations between Alice and Bob of the form (1) when q_A is chosen such that $q_A + (1 - q_A)\eta_c = \eta_l$.

At present, the asymptotic secret-key rate R of any DIQKD protocol in which the key is established by one-way classical communication reconciliation techniques is determined by the best-known lower bound of Arnon-Friedman et al. [7], which is valid for most general eavesdropping attacks and reads:

$$R \geq \tilde{R} = H(A|E) - H(x^*|y^*). \quad (2)$$

Here $H(x^*|y^*)$ is the classical conditional Shannon entropy between Alice and Bob outputs when choosing any inputs (x^*, y^*) used for the key and $H(A|E)$ is the conditional von Neumann entropy between Alice’s output and the quantum state in the hands of the eavesdropper, Eve. Crucially, the Bell violation observed by Alice and Bob allows them then to estimate (lower-bound) $H(A|E)$ without making any assumptions about Eve [2–7].

However, as Eq. (2) applies to any attack, we can explicitly evaluate it for the strategy discussed above. Returning to correlations (1) that incorporate losses, we compute the conditional entropy $H(x^*|y^*)$. For the sake of simplicity, we perform this calculation for the common case of two-output measurements, while the correlations between Alice and Bob define a perfectly correlated bit in the absence of losses, so that $H(x^*|y^*) = 0$ for $\eta_l = 1$. For the above simple attack, we easily see that $H(A|E) = q_A = (\eta_l - \eta_c)/(1 - \eta_c)$ for $\eta_l \geq \eta_c$, as Eve has then complete knowledge with probability $(1 - q_A)$ and complete uncertainty with probability q_A . In contrast, for $\eta_l \leq \eta_c$ the attack of Eve works all of the time, so that then $H(A|E) = 0$. Within the inset of Fig. 1 we plot explicitly both these conditional entropies for $n_k = 1$ and $m = 2$.

In Fig. 1, we depict the critical values of the local efficiency, η_l^* , at which the key rate computed through (2) becomes zero as a function of the number of bases, n_k , used to construct the key. Note that based on such an attack, the tolerable local efficiency is forced to be at least 85.7% for any DIQKD

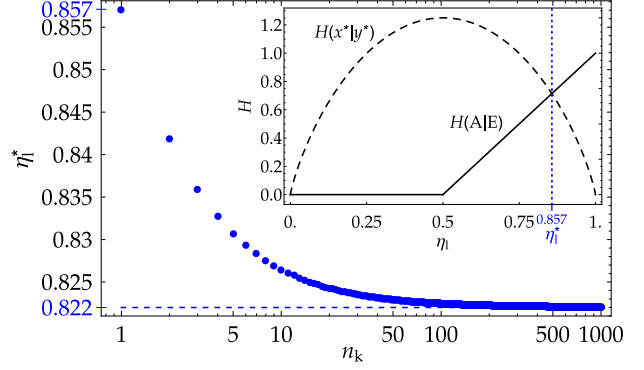


Figure 1: **Lower bound on critical local efficiency, η_l^* , for DIQKD** as a function of the number of measurement settings, n_k , that are used to generate the key. For each n_k and any $\eta_l < \eta_l^*$ below the corresponding value (blue dot), there exists a simple attack based on the eavesdropping strategy introduced in Ref. [45] that prevents any protocol based on two-party correlations (1) from being secure. The most and the least optimistic critical efficiencies for $n_k \rightarrow \infty$ and $n_k = 1$, respectively, are also marked in blue. For $n_k = 1$, the conditional entropies whose difference determines the key rate (2) are explicitly shown in the inset.

scheme with $n_k = 1$, e.g. the ones of Refs. [36, 41–44] employing one-way communication. Moreover, the above simple attack—with its corresponding critical local efficiencies applying to *any* DIQKD protocol and any Bell inequality which uses the security proof of Ref. [7]—demonstrates that even in the unrealistic case of users employing an infinite number of bases $n_k \rightarrow \infty$ (see Fig. 1) the local efficiencies must necessarily exceed 82.2% for a positive key rate to be possible.

In view of these results, we expect that high efficiencies will inevitably be needed in DIQKD protocols, and the only solution we foresee is to develop even more efficient photon sources [46–48], better detectors [49–52] and improve all the couplings within optical implementations to sufficiently decrease losses within the users’ laboratories. Nevertheless, we expect Bell experiments with local losses of the order of 90% to be within reach in the near future. In this work, we work under this assumption, which is currently essential for any existing DIQKD implementation.

2.2 Transmission losses

The second type of losses occur while photons propagate outside the labs and are quantified by the *transmission efficiency*, η_t , of the channel connecting the users. In principle, they constitute the main hurdle for long-distance DIQKD, as η_t decreases rapidly with distance, e.g. exponentially when transmitting signals over optical fibres. Moreover, even if fibre technology progresses, the exponential increase of losses with distance will remain, due to unavoidable light absorption and scattering. However, contrary to lo-

cal losses, transmission losses can be completely overcome by adopting a carefully constructed protocol. A viable route to do so is to record an additional outcome, denoted by \checkmark , indicating in a heralded way that the photons did not get lost [35, 36, 53]. Then, \checkmark assures that the required quantum state was successfully transmitted between Alice and Bob and the Bell test can be performed. If the heralding outcome is causally disconnected from the choices of measurement settings x, y by Alice and Bob during each round of the protocol (see Fig. 2), transmission losses become irrelevant with respect to the security of the protocol, affecting only the key rate. In fact, the heralding signal, when causally disconnected from the choice of measurements, can simply be interpreted as a probabilistic preparation of the required state which does not affect a Bell test, nor any protocols based on it.

The heralding process can in principle be implemented with the help of a quantum non-demolition (QND) measurement allowing the number of photons to be measured without disturbing the quantum state [54]. QND photon measurements are, however, challenging, requiring e.g. unrealistic optical non-linearities. The solution is to replace them with optical linear circuits that achieve the same goal in a probabilistic fashion [55, 56]. The heralding signal \checkmark is then provided by a particular detection pattern in the linear optics circuit indicating, as for the QND measurement, that the outputs produced by the Bell test are valid.

Within the *side-heralding* (SH) scenario depicted in Fig. 2(a), the circuit is performed by one of the users who records the rounds in which the positive heralding pattern, \checkmark , has occurred, so that only these are later used for key extraction. In contrast, in the *central-heralding* (CH) scenario the heralding is performed outside of the users labs, at a central station (resembling the entanglement swapping configuration [57]), by a third party who then publicly announces which rounds should be considered successful, as illustrated in Fig. 2(b). In either case, the heralding scheme should be causally disconnected from the measurements in the Bell test. This condition is more natural in the CH scheme, within which it is naturally assured by the lack of information leakage from the secure user labs. On the contrary, in the SH configuration it becomes the responsibility of the user holding the heralding device within their lab, who must then, e.g. ensure that the heralding signal occurs before a random choice of measurement is made¹. In any case, the heralding signal should work as the ideal QND measurement and assure that, up to the leading order, transmission losses have no effect on the heralded Bell violation.

The importance of this requirement is best un-

¹Ideally, each user possesses an independent source of private randomness [58].

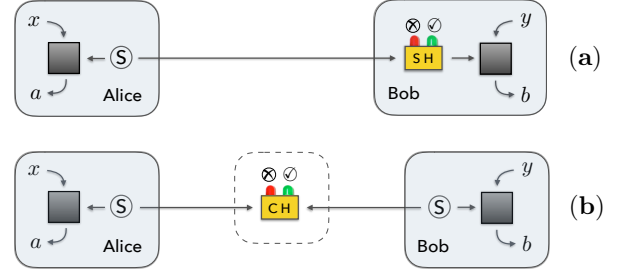


Figure 2: **Efficient heralding schemes for DIQKD.** Alice and Bob are located at isolated labs (shaded regions) from which they control information leaks. They locally use sources S , to distribute a quantum state between their labs and perform on it randomly sampled measurements labelled x and y , producing outcomes a and b . The measurement devices are treated as black-boxes that yield a joint probability distribution $\mathbf{p} = \{P(ab|xy)\}_{abxy}$ compatible with the laws of quantum physics. A *heralding scheme* is implemented, such that, given its positive outcome \checkmark , the resulting $p(ab|xy\checkmark)$ shared between Alice and Bob becomes effectively independent of the finite transmission efficiency. In the *side-heralding* (SH) scenario, (a), this is achieved by one of the users performing a (probabilistic) quantum non-demolition measurement (QND) within their isolated lab that verifies the arrival of the distributed state, without disturbing it. In the *central-heralding* (CH) scheme, (b), the heralding is performed by a third party that later publicly announces the successful rounds that should be used during the protocol.

derstood by considering existing proposals for photonic DIQKD that do not satisfy it, such as the schemes using a noiseless qubit amplifier [36] or entanglement swapping relays [41–43]. In all these schemes, entanglement between users is distributed using spontaneous parametric down-conversion [33] (SPDC) sources—a probabilistic process in which multi-photon pair creation also takes place. For the sake of argument, let us consider the state produced by the SPDC to read: $|0\rangle\langle 0| + \bar{p}|\psi_{AB}\rangle\langle\psi_{AB}|$; after, without loss of generality, ignoring its normalisation and the higher-order terms in \bar{p} , i.e. the spurious contributions arising when more than one photon-pair is created within the process—see App. A. For all the schemes, the state shared by the users after a successful heralding takes a general form (up to irrelevant normalisation):

$$\rho_{AB|\checkmark} = |0\rangle\langle 0| + \lambda \eta_t \bar{p} |\psi_{AB}\rangle\langle\psi_{AB}| + \dots, \quad (3)$$

in which the detrimental terms of order \bar{p} that yield deviations from the target $|\psi_{AB}\rangle$ may also be omitted. The parameter $\lambda > 0$ above is determined by the particular heralding scheme [36, 41–43], while η_t is the transmission efficiency dependent on the distance between the users.

The key point is to notice that the contribution of the maximally entangled state, $|\psi_{AB}\rangle$, in Eq. (3) occurs at a higher order in \bar{p} than the vacuum contribution and is influenced differently by the pres-

ence of transmission losses. Thus, for any fixed λ , the Bell violation strongly depends on η_t . That is, contrary to when performing an ideal QND measurement, transmission losses not only affect the key rate but also the protocol security. In optical fibres, η_t vanishes exponentially with the separation distance L ($\eta_t = e^{-L/L_{\text{att}}}$, with typical values of the attenuation length $L_{\text{att}} \approx 20$ km), and so the heralded state (3) approaches the vacuum exponentially with L , while rapidly ceasing to produce large enough Bell violations for DIQKD to be possible [44]. In particular, this implies that in all such protocols there is always a critical distance at which the protocol ceases to be secure.

For the sake of clarity, we provide some simple estimations that make this point more explicit for the scheme based on the qubit amplifier of Ref. [36]. As discussed also in App. B, if one approximates for simplicity $1 - \bar{p} \approx 1$, the state after heralding can be put in the form of Eq. (3) with $\lambda = T/(1 - T)$, where T is the transmittance of the beam-splitter used in the qubit amplifier for the heralding process [36]. Even if quite optimistic, we can take a value of $T = 1 - 10^{-2}$, which gives $\lambda \approx 10^2$. This severely affects the key rate, which is a function of $1 - T$, but here we focus on the protocol security.

For any protocol based on the violation of the CHSH inequality $S_{\text{loc}} \leq 2$ (e.g. the one of Ref. [36]), the heralded state (3) must lead to

$$S \leq \frac{1}{1 + \lambda \eta_t \bar{p}} (2 + \lambda \eta_t \bar{p} 2\sqrt{2}). \quad (4)$$

Following Ref. [2], the inequality (4) allows one to lower-bound the term $H(A|E) \geq 1 - \chi(S)$ in Eq. (2), where $\chi(S) = h[(1 + \sqrt{(S/2)^2 - 1})/2]$ is the binary entropy. On the other hand, for key-generation rounds, the conditional entropy $H(x^*|y^*) = 1 - h[\bar{\lambda}]$ where $\bar{\lambda} = \lambda \eta_t \bar{p} / (1 + \lambda \eta_t \bar{p})$ is the effective probability of sharing the target state $|\psi_{AB}\rangle$, given the state (3). Putting all these terms together, using the expression for the losses as an exponential function of the distance, and taking an optimistic value of $\bar{p} = 10^{-2}$ for SPDC [23, 24], the key rate (2) vanishes already for distances of approximately one attenuation length, $L_{\text{att}} \approx 20$ km. This critical limit on user separation can be improved by taking even smaller values of T or larger values of \bar{p} , but the problem still remains: for any given values, the weight of the entangled part in the state obtained after successful heralding always decreases exponentially with distance.

The key rates reported in Ref. [36] are much higher than those obtained in the above. This arises due to the fact that the authors of Ref. [36] make additional assumptions on the attacks available to the eavesdropper (see for example the Supp. Mat. of Ref. [36] and also the discussion in Ref. [44]). Using these assumptions, they derive a different bound on the key rate as a function of an observed CHSH Bell violation

and the rates at which one or both parties observe inconclusive events. The same bound was later used in the protocols of Refs. [41–43]. Unfortunately, it is unclear whether these assumptions, and corresponding rates, do not imply a loss of generality. In fact, for a slightly different situation in which losses only occur for one of the observers, these assumptions and corresponding bounds can be explicitly proven not to hold: for some value of the losses they predict a strictly positive secret-key rate, while it is possible to derive an explicit eavesdropping attack that breaks the protocol. The details of this attack are shown in App. C. This analysis implies that the assumptions used in Ref. [36], and later in Refs. [41–43], do not hold in full generality and, therefore, it is unclear to what extent the secret-key rates reported in these works are valid.

In what follows, we propose two DIQKD architectures based on single-photon sources [25] that crucially do not suffer from the above problems. They are designed such that up to the leading order a pure entangled state is shared between the users upon successful heralding – independent of their separation (or transmission losses). Our protocols thus behave as the ideal QND measurement and allow high key rates to be maintained over large communication distances. One of the schemes relies solely on single photon sources and a CH-based implementation. Since single-photon sources are still an expensive resource compared to widely used SPDC sources, we furthermore consider a SH-based scheme in which both source-types are used in conjunction. In order to maintain generality and a degree of comparison with the SPDC framework [33], each single-photon source is modelled to produce a quantum state that, when ignoring normalisation (see also App. A), reads $\sigma_{\text{SP}} = \sum_{n=1}^{\infty} p^{n-1} |n\rangle\langle n|$ in the photon-number basis, containing an infinite tail of high-order contributions whose probability is parametrised by p .

3 DIQKD schemes with single-photon sources

The *SH scheme* requires Bob to produce two single photons with orthogonal polarizations H and V , while Alice has access to entangled photon-pairs produced by an SPDC source. It is inspired by the qubit-amplifier implementation of Pitkanen et al. [44], as shown in Fig. 3(a). Bob’s photons enter a beam-splitter (BS) of transmittance T . Then, the reflected light component passes through a half-waveplate (HWP) before being detected in conjunction with Alice’s transmitted photons via a partial Bell-state measurement (BSM) depicted by the dashed region. The outcome of the BSM, c , signifies whether the required heralding pattern, $c = \odot$, has occurred, corresponding to two detector clicks that represent

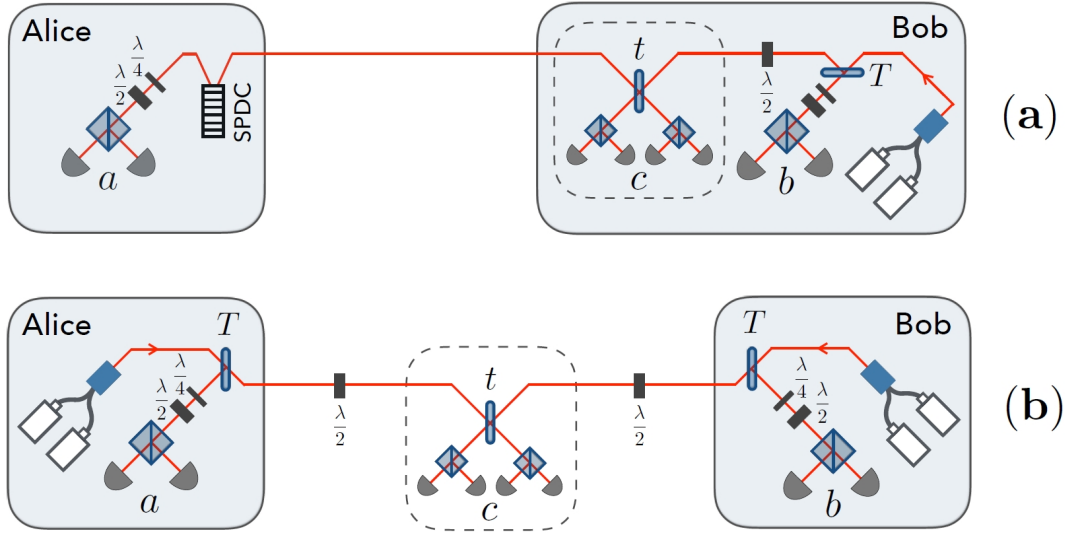


Figure 3: **DIQKD schemes with single-photon sources.** (a): *Side-heralding (SH) scheme employing two single-photon sources.* The SPDC source is kept close to Alice to avoid transmission losses on her side. Two single photons held by Bob and encoded in orthogonal polarizations impinge a BS of transmittance $T \approx 1$ located in his lab (shaded region). The reflected mode is then jointly analysed with the system received from Alice by a partial Bell-state measurement (BSM, dashed region) consisting of: a partial BS of transmittance t , polarizing-BSs (split squares) and binary on/off photodetectors (half-circles). (b): *Central-heralding (CH) scheme employing two single-photon sources.* Both Alice and Bob project two single photons encoded in orthogonal polarizations onto BSs of transmittance $T \approx 0$ situated in their labs. A partial BSM is conducted this time at the central station on the combined polarization components arriving from Alice and Bob after being passed through HWP's ($\frac{\lambda}{2}$). In both schemes, the users apply their choice of the measurement settings x and y on the output modes by means of a polarization analyser—a sequence of a quarter-wave plate ($\frac{\lambda}{4}$), HWP, polarizing BS and two binary detectors.

simultaneous detection of orthogonal polarizations.

Provided that the BS transmittance is kept close to one ($T \approx 1$), \checkmark occurs only when exactly one photon is transmitted by the BS while the other photon is reflected, and the single photon-pair term of the state produced in the SPDC by Alice reaches the BSM. In this manner, the photons distributed to Alice and Bob are prepared with orthogonal polarizations, although the information about their concrete polarization is erased by the partial BSM. The resulting state shared by Alice and Bob conditioned on \checkmark corresponds to a partially (polarization-) entangled two-qubit state with asymmetry dictated by the BSM transmittance parameter t (in an unnormalised form):

$$\rho_{AB|\checkmark}^{(SH)} = \frac{\eta_t T (1 - T)}{8} |\psi_{AB}^t\rangle \langle \psi_{AB}^t| + O(\bar{p}), \quad (5)$$

where \bar{p} parametrises the probability to produce multiple pairs in the SPDC process of Alice (see App. D). The target state $|\psi_{AB}^t\rangle = |\psi_{AB}^t\rangle + t|\phi_{AB}^t\rangle$ in Eq. (5) is a superposition of Bell states given, in second quantization, by $|\psi_{AB}^t\rangle = \frac{1}{\sqrt{2}}(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger)|0\rangle$ and $|\phi_{AB}^t\rangle = \frac{1}{\sqrt{2}}(a_H^\dagger b_H^\dagger - a_V^\dagger b_V^\dagger)|0\rangle$.

The CH scheme depicted in Fig. 3(b) requires both Alice and Bob to produce two single photons with orthogonal polarizations H and V , inspired by the entanglement distribution scheme of Lasota et al. [59]. The photons produced on each side impinge separate BSs of low transmittance ($T \approx 0$) and, thus, reach

the central station with low probability. The heralding is again provided by a partial BSM, performed now by a third party, after passing both incoming beams through separate HWP's. The signal \checkmark is observed only when each party transmits exactly one single photon and in such a case the reflected photons kept by Alice and Bob are again in a partially (polarization-) entangled state with asymmetry determined by the transmittance t of the partial BSM performed at the central station (see App. D):

$$\rho_{AB|\checkmark}^{(CH)} = \frac{\eta_t T^2 (1 - T)^2}{4} |\psi_{AB}^t\rangle \langle \psi_{AB}^t| + O(p). \quad (6)$$

Unlike previous proposals, see Eq. (3), in the above two schemes the vacuum terms do not emerge after heralding. Moreover, the unnormalised states (5) and (6), to first significant order, are pure and proportional to the transmission efficiency η_t . This guarantees that, after normalisation, the states are independent of η_t (to first order). This, and the use of single-photon sources instead of SPDC, are the crucial ingredients that allow us to achieve significantly higher secret key rates at larger distances than previous proposals.

The second advantage of our schemes is that, by adjusting the transmittance t of the partial BSM, the entanglement of the target state $|\psi_{AB}^t\rangle$ can be continuously tuned between the maximally entangled ($t = 0$) and product ($t = 1$) extremes [13]. This can then be used, in particular, to improve the local ef-

DIQKD Scheme:	Side-heralding (SH)	Central-heralding (CH)
<i>Critical local efficiency η_1^* (diqkd)</i>	94.9%	94.3%
<i>Critical local efficiency η_1^* (nonloc.)</i>	74.3%	69.2%
<i>Noise robustness (nonloc.)</i>	31.2%	35.7%
<i>Secret key per heralded round (bit fraction ≤ 1)</i>	0.82	0.95

Table 1: **Performance of DIQKD schemes.** Critical local efficiencies, η_1^* , only above which the secret key can be distributed in a fully device-independent fashion, compared with ones above which the shared correlations exhibit nonlocality. For perfect local efficiencies ($\eta_1 = 1$), robustness to mixing the joint probability distribution with a maximally uncorrelated one is listed, as well as the bit fraction of the secret key generated per successfully heralded round, equal to one in the ideal case. The probability of producing a single photon or an SPDC photon-pair is assumed as $p = \bar{p} = 10^{-4}$ for each source.

ficiencies, η_1 , required to meet the security requirements.

We notice that it is possible to reduce the number of single photon sources in our schemes by using a single source emitting a temporal stream of photons. This would require, however, the stream to be demultiplexed either by active optics (which would add extra noise) or probabilistically by passive elements (which would decrease the final heralding rate).

4 Computing key rates in heralded schemes

In standard DIQKD protocols, Alice and Bob measure their particles. A subset of these measurements is publicly announced so that the users can count how many times different outcomes (a , b) are obtained for the different combinations of inputs (x , y). From this information, they compute the amount of achievable secret key and, if positive, distil it by means of classical post-processing [60] from the remainder of data being shared, specifically, from particular pre-designed measurement settings (x^* , y^*) [2–4]. As mentioned, in the asymptotic limit of infinitely many rounds, the attainable key rate is given by Eq. (2), which constitutes the best known lower bound, that, crucially, is valid for the most general eavesdropping attacks [7].

Calculating exactly $H(A|E)$ in Eq. (2), for a given observed correlation \mathbf{p} or Bell inequality violation, optimising over attacks of Eve, turns out to be extremely hard. The problem has only been solved for the CHSH inequality [2], the simplest of all Bell inequalities. Here, we use a lower bound on $H(A|E)$, which in turn provides a lower bound on the key rate, computable for any type of correlations. It is obtained by replacing the von Neumann entropy in Eq. (2) by the min-entropy [4]. This quantity is then directly connected to the guessing probability, $G_{\mathbf{p}}(x^*)$, for Eve to correctly guess Alice’s output when she performs the measurement x^* . It can be computed for any Bell correlations exhibited by \mathbf{p} by means of semi-definite programming, as explained in App. E. The resulting bound on the key

rate (2), which has already appeared in previous security proofs [4, 5], reads

$$R \geq \tilde{R} \geq R^\downarrow = -\log_2 G_{\mathbf{p}}(x^*) - H(x^*|y^*). \quad (7)$$

In an ideal scenario with two outcomes, there are no errors between Alice and Bob, $H(x^*|y^*) = 0$, and Eve has no information about Alice’s outputs, $G_{\mathbf{p}}(x^*) = 1/2$, so that $R = R^\downarrow = 1$. Because of its ease of computation, R^\downarrow is the quantity used here to estimate attainable key rates of the implementations proposed.

When considering protocols that incorporate a heralding stage depending on an outcome c , with rounds occurring at a repetition rate ν_{rep} , we quantify the effective key rate of secret bits certified per time-unit as:

$$K = \nu_{\text{rep}} P(c = \odot) R^\downarrow, \quad (8)$$

where $P(c = \odot)$ is the probability of successful heralding in each round.

5 Performance of the SH and CH schemes

As a result, we may quantify the optimal DIQKD-performance of the CH and SH schemes depicted in Fig. 3, by conducting an unconstrained nonlinear maximisation of K in Eq. (8) over all adjustable parameters. In particular, for each of the schemes, we optimise over the source parameters p and \bar{p} , transmittance values T and t , as well as polarization angles specifying the user measurements. Still, we ensure $p, \bar{p} \approx 0$ and $T \approx 1$ (or $T \approx 0$) in case of the SH (or CH) scheme, so that the distributed quantum states can be truncated at a finite order in p , \bar{p} and $1 - T$ (or T). Nonetheless, in order to maintain security we bypass such a truncation by giving full control to the eavesdropper over the higher-order terms that are neglected. Moreover, the critical noise parameters can then also be determined by similar optimisation procedures—conducted while increasing the noise until the key rate (8) cannot be made strictly positive. Explicit details about these optimization steps are given in Apps. E, F and G.

We summarise the performance of the SH and CH schemes in Table 1. Although the SH scheme is simpler, requiring only two single-photon sources, its performance is worse than the CH scheme for all figures of merit considered. From here onwards, we thus focus on the CH scheme, which defines the ultimate experimental requirements for DIQKD to be possible within our approach. In what follows, we show that this scheme offers reasonable levels of robustness against all relevant noise parameters.

The resistance to noise is estimated using a simple noise model, in which the ideal correlations are mixed with white-noise correlations with weight $1 - v$ and v , and perfect local efficiency ($\eta_l = 1$) is assumed. The CH scheme yields nonlocal correlations up to $v = 35.7\%$ level of mixing. Concerning imperfection of the single-photon sources, for a realistic value of multi-photon generation of $p = 10^{-4}$ (c.f. [32]) the CH scheme generates up to 0.95 secret bits per (successfully) heralded round—achieving close to the ultimate limit of 1 secret bit, applicable in a perfectly noiseless scenario [61]. The critical local efficiencies, η_l^* for the nonlocality to be observed are very close to the ultimate bound of Eberhard [13], $\eta_l \geq 66.6\%$, which can be approached due to the ability to prepare pure partially entangled two-qubit states within both the SH and CH schemes.

Most importantly, employing the CH scheme for DIQKD, our work predicts that positive key rates can be generated independently of the separation between Alice and Bob, as long as the effective local efficiency, η_l , for each of the user labs is higher than 94.3%. Assuming η_l to be the product of the efficiencies of: photon extraction from each single-photon source employed (η_{ls}), transmission between the sources and detectors involved (η_{lt}), and detection (η_{ld}); fully secure DIQKD is possible as long as $\eta_l = \eta_{ls}\eta_{lt}\eta_{ld} \geq 0.943$ can be attained by each user.

Taking, for instance, $\eta_l = 95\%$ (see also Fig. 4), the secret key can be securely distributed over large distances while completely avoiding the transmission losses. In particular, assuming in Fig. 4 for the CH scheme: realistic $\eta_t = e^{-L/L_{\text{att}}}$ with $L_{\text{att}} = 22$ km [36], the lab beam-splitters to exhibit transmission $T \approx 10^{-3}$, and each of the sources employed to be producing photons at 100 MHz rate with $p = 10^{-4}$ [32]; a key rate of 1 bit/s can be attained over approximately 50 km. In Fig. 4, we consider also the SH scheme, for which we then assume the SPDC source to produce entangled photons also at 100 MHz rate with $\bar{p} \approx 10^{-4}$ —both theoretically within current technological reach [23, 24, 62]—but also ensure $T \approx 1 - 10^{-3}$ to make the comparison fair.

However, let us note that the corresponding values of key-rates are primarily dictated by the factor $K \propto \nu_{\text{rep}} P(c = \textcircled{Q})$ appearing in Eq. (8) with the successful-heralding probability effectively equal to T^2 and $\bar{p}(1 - T)$ at $L = 0$ for the CH and

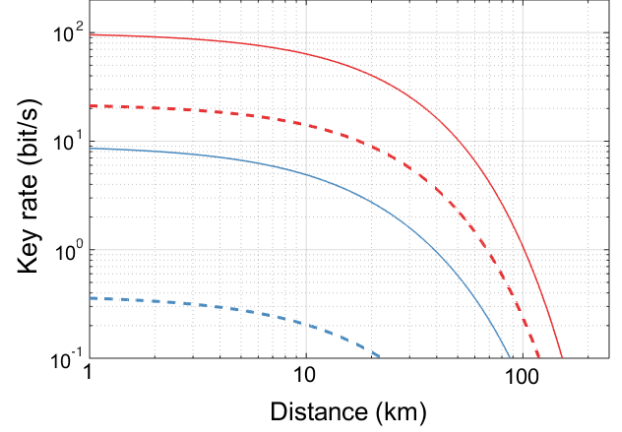


Figure 4: **DIQKD key rates attained with 95% (blue) and 96% (red) local efficiencies.** In each case, the solid (dashed) curve represents the key rate in bits per second attained by the CH (SH) scheme. Each key rate is optimised over all adjustable physical parameters, yet in the case of the single-photon sources impurity parameter, p , its lowest possible value is always favoured. Here, we fix $p = 10^{-4}$, and consider the repetition rate of photon extraction for each source to be 100 MHz [32].

the SH scheme, respectively. In particular, as for the single-photon sources we take $p > 0$ to account solely for multi-photon events, its impact on the key rates is negligible. Although in our analysis we were motivated to use the least number of single-photon sources, under such an assumption the limiting dependence of key rates on how well $T \approx 0$ (or $T \approx 1$) could, in principle, be avoided by creating more photons and performing within each lab extra (local) pre-heralding [55, 56], which must importantly assure a polarisation-entangled photon pair to be distributed. When employing multiple SPDC sources such an approach may seem to be even less efficient [63–65], however, rapid development of solid-state emitters capable of producing on-demand entangled photons could provide a breakthrough [66–68].

6 Conclusions and outlook

Two proposals for photonic implementations of DIQKD schemes have been given here. They make use of side- or central-heralding, and utilise two or four single-photon sources, respectively. They are capable of maintaining security despite arbitrary transmission losses, and distribute keys over large distances given sufficiently high local efficiencies.

The analysis proves the proposed photonic architectures to be almost optimal from the implementation perspective, as they allow to nearly perfectly compensate for the impact of finite transmission, so that devices can operate independently of the distance separating the users. In contrast, as shown to be generally demanded within the context of DIQKD, being a feature of current state-of-the-art security

proofs [7], the requirements on local efficiencies for the protocols remain to be stringent. Hence, an important question that remains open is whether these demanding requirements can be improved by developing more elaborate proofs that, in particular, allow the users to perform two-way communication during the protocol rather than only one-way error correction that is typically assumed [2–7]. Unfortunately, recent progress in this direction has indicated that not much room for improvement may be available in this respect without jeopardising the full security [69, 70].

Another important future direction is to improve the key-rate analysis presented here, while accounting in more detail for the limitations of particular photonic components being employed [71]. On the one hand, an explicit study of the impact of detector dark counts would be valuable, even though our noise-robustness analysis suggests these not to play a major role (see the values presented in Table 1). On the other hand, the protocol repetition-rates have been assumed to be primarily dictated by the capabilities of the photon sources employed [32, 62], while ignoring, e.g. the finite dead-time of the binary detectors.

Nonetheless, while the requirements on local efficiencies for the proposed protocols are currently challenging, based on the rapid technological improvement and anticipated capabilities of single-photon sources [46–48] and detectors [49–52], we hope that the demands on fully secure DIQKD implementations presented already here will be fulfilled in the future.

Note Added. After making this work publically available online at [arXiv:1803.07089](https://arxiv.org/abs/1803.07089) [quant-ph], an alike study of CH and SH schemes for DIQKD has been released [72], which by focusing on the Bell violation of the CHSH inequality arrives at slightly higher requirements for local efficiencies but goes beyond the asymptotic key-rate analysis—see also a very recent work [73] that develops finite-key analysis for DIQKD. Moreover, the model of the CH scheme has been developed and explicitly verified against an experimental implementation within the scenario in which Alice and Bob possess an SPDC source of entangled photons each (rather than two single-photon sources) [74]. Although the theoretical predictions have been demonstrated to accurately reproduce the observed correlations, these currently do not exhibit Bell violations strong enough for DIQKD, as the corresponding local efficiencies do not yet reach the stringent regime of $\eta_l \gtrsim 95\%$ indicated by our work.

Acknowledgments

We thank Rotem Arnon-Friedman, Mikołaj Lasota, Stefano Pironio and Nicolas Sangouard for helpful discussions. This work was supported by the ERC CoG QITBOX and AdG CERQUTE, Spanish

MINECO (Severo Ochoa SEV-2015-0522), Fundacio Cellex and Mir-Puig, the AXA Chair in Quantum Information Science, the Generalitat de Catalunya (SGR1381 and CERCA Program), the Royal Society (URF UHQT), the EU Quantum Flagship projects QRANGE and CiviQ, as well as by the Foundation for Polish Science under the “Quantum Optical Technologies” project carried out within the International Research Agendas programme co-financed by the European Union under the European Regional Development Fund.

A States produced by the SPDC and single-photon sources

The process of spontaneous parametric down-conversion [33] (SPDC) producing two-mode polarisation entangled photons is described by the Hamiltonian $\hat{H} = i\kappa(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger) + h.c.$, where a_H^\dagger , a_V^\dagger , b_H^\dagger and b_V^\dagger are the bosonic creation operators of the two spatial modes a and b , with H and V denoting their orthogonal polarizations. Rewriting \hat{H} with help of the $\text{su}(1,1)$ algebra generators, i.e. ones that obey $[L_-, L_+] = 2L_0$ and $[L_0, L_\pm] = \pm L_\pm$, it is straightforward to verify that the state produced via the SPDC reads [75]:

$$|\Psi_{\text{SPDC}}\rangle = e^{-i\hat{H}t}|0\rangle = e^{\tau(L_+ - L_-)}|0\rangle \quad (9)$$

$$= (1 - \tanh^2 \tau) e^{\tanh \tau L_+} |0\rangle, \quad (10)$$

where $L_+ = L_-^\dagger = a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger$, $|0\rangle$ denotes the vacuum state of all modes, while $\tau = \kappa t > 0$ can be assumed to be real.

Moreover, as throughout this work we consider photonic schemes based on (binary, on/off) photodetection, the state Ψ_{SPDC} should be interpreted as an incoherent mixture of different photon-number states due to lack of a global phase reference. Hence, defining $q = \tanh^2 \tau$ as the effective parameter of the SPDC process, one arrives at the expression:

$$\varrho_{\text{SPDC}} = (1 - q)^2 \sum_{n=0}^{\infty} (n+1) q^n |\Psi_n\rangle \langle \Psi_n|, \quad (11)$$

where $|\Psi_n\rangle = \frac{1}{n! \sqrt{n+1}} L_+^n |0\rangle$ is the pure state obtained when n photon-pair excitations occur during the down-conversion.

Nonetheless, for simplicity and the purpose of our work, we redefine the state (11) in an unnormalised fashion as,

$$\rho_{\text{SPDC}} = \sum_{n=0}^{\infty} \frac{n+1}{2^n} \bar{p}^n |\Psi_n\rangle \langle \Psi_n| \quad (12)$$

$$= |0\rangle \langle 0| + \bar{p} |\Psi_1\rangle \langle \Psi_1| + O(\bar{p}^2), \quad (13)$$

such that $\text{Tr}[\rho_{\text{SPDC}}] = 1/(1 - 2\bar{p})^2$, and so that the parameter $\bar{p} = 2q$ can now be directly associated with

the contribution of the desired singlet:

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} (|1_H\rangle_a |1_V\rangle_b - |1_V\rangle_a |1_H\rangle_b) \quad (14)$$

$$= \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle). \quad (15)$$

Experimentally, the parameter \bar{p} is kept small (below 10^{-2}) and may be adjusted with squeezing techniques [23, 24]. Although large values of \bar{p} increase the production rate of the target maximally entangled two-photon states, $|\Psi_1\rangle$, they also increase the relative contribution of spurious higher-order terms, $|\Psi_{n>1}\rangle$, to the SPDC process.

On the other hand, as stated in the main text, whenever the single-photon (SP) sources [25] are used, we represent states they produce in an analogous unnormalised, $\text{Tr}[\sigma_{\text{SP}}] = 1/(1-p)$, manner as:

$$\sigma_{\text{SP}} = \sum_{n=1}^{\infty} p^{n-1} |n\rangle\langle n| \quad (16)$$

$$= |1\rangle\langle 1| + p|2\rangle\langle 2| + O(p^2), \quad (17)$$

where the desired single-photon is then produced at the *zeroth* order in p ($\approx 10^{-4}$ in current experiments [32])—in contrast to the SPDC process (12) in which the target photon-pair (15) occurs at the *first* order in \bar{p} in Eq. (13).

Finally, let us emphasise that throughout this work we perform calculations for all the schemes beyond their expected ideal working-order in \bar{p} and p , i.e. by performing truncations of (13) and (17) at higher orders. Still, it is crucial to mention that, when we compute the results (key rates and figures of merit presented in Table 1 of the main text), we nevertheless bypass such a truncation by assuming that higher-order terms (those which were dropped) are controlled by the eavesdropper to her own benefit. We give the details of this technique in App. F below.

B Heralded state produced by the qubit amplifier of Gisin et al. [36]

The original scheme of Ref. [36] is of the SH type (see Fig. 2(a) of the main text) and consists of an SPDC source held by Alice and two single-photon sources (emitting photons in H and V polarisation modes) held by Bob. For the sake of the argument, let us assume that all the sources do not produce multiple pairs, which is only beneficial for the scheme.

The initial composite state of Alice and Bob before communication and amplification reads [36]:

$$[(1-\bar{p})|0\rangle\langle 0| + \bar{p}|\Psi_1\rangle\langle\Psi_1|] \otimes |1_H\rangle\langle 1_H| \otimes |1_V\rangle\langle 1_V|. \quad (18)$$

Bob's photons enter a beam-splitter of transmittance T , so that the reflected mode can then be combined

with the mode received from Alice within an implementation of the Bell-state measurement (BSM). As a consequence, the final unnormalized state that is shared by Alice and Bob, conditioned on the (heralding) success of the BSM performed by Bob, reads:

$$(1-\bar{p})(1-T)^2|0\rangle\langle 0| + \bar{p}\eta_t T(1-T)|\Psi_1\rangle\langle\Psi_1| + \dots, \quad (19)$$

where we have already ignored all irrelevant terms that do not yield any correlations apart from the vacuum—which occurs with probability proportional to $(1-T)^2$, since both of Bob's photons are reflected and detected. The second term in Eq. (19) corresponds to the case when Alice produces the singlet (15), which is transmitted with probability η_t , and only one of Bob's photons is reflected. One can see that Eq. (19) is of the form of Eq. (3) in the main text with the effective $\lambda = T/(1-T)$.

Such a feature will always emerge as long as the singlet (target) state is proportional to η_t , while the vacuum component remains unaffected by the finite transmission efficiency. In particular, it naturally generalises to scenarios based on 'entanglement-swapping' or 'teleportation' [41–43] and hence, as explained in the main text, constitutes the main limitation of all these schemes. The only exception is the 'quantum-relay'-based scheme proposed in Ref. [41] that, however, due to SPDC sources being employed yields a conditional state still containing undesired terms in apart from the singlet contribution in Eq. (5).

C Secret-key rate under losses

In this appendix, we present a rather natural scenario in which the bound on the key rate derived by Gisin et al. [36] can be proven not to hold. In the supplemental material of Ref. [36], the situation is studied in which Alice and Bob implement lossy measurements on an entangled state. The goal is to establish an upper bound on the information that an eavesdropper can possess about the outcomes used for generation of the secret key, given that the non-detected events have already been discarded.

A bound based only upon the statistics of the conclusive events is not possible, as it would open the detection loophole. In Ref. [36] a method is given for bounding Eve's knowledge about the conclusive correlations, based upon the full (lossy) correlations. The main result, see Eq. (10) in their work, is the following bound on the mutual information, $I(A : E) = H(A) - H(A|E)$, between Alice and Eve:

$$I(A : E) \leq I_E(S_{\text{cc}}, \mu) = (1-\mu) \chi\left(\frac{S_{\text{cc}} - 4\mu}{1-\mu}\right) + \mu. \quad (20)$$

Here, μ is a parameter defined by the ratio of the rates of conclusive-conclusive events, μ_{cc} , and conclusive-inconclusive events, μ_{ci} and μ_{ic} , from Alice's and

Bob's perspective, respectively, and reads

$$\mu = \frac{\mu_{ci} + \mu_{ic}}{\mu_{cc}}. \quad (21)$$

The parameter S_{cc} , on the other hand, denotes the value of the CHSH inequality when computed *only* from the conclusive events. Finally, the function

$$\chi(S) = h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) \quad (22)$$

with $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ has already been employed in the main text, see below Eq. (4), and follows from Ref. [2]. For what follows, the property to remember is that $\chi(S) < 1$ if $S > 2$. We also emphasise that the bound (20) depends on the lossy correlations: while the Bell parameter used in I_E in Eq. (20) is estimated only from the conclusive events, I_E depends also on the rates of conclusive and inconclusive events via the parameter μ .

Let's apply the bound (20) to a situation in which losses only appear on Alice's side. The corresponding correlations, \mathbf{p}^m , between Alice and Bob then read analogously to Eq. (1) of the main text:

$$\begin{aligned} P^m(ab|xy) &= \eta_1 P(ab|xy) \\ P^m(\phi b|xy) &= (1 - \eta_1) P_B(b|y), \end{aligned} \quad (23)$$

where again a and b refer only to conclusive 'detection' events, while P_A and P_B denote the marginal probabilities detected by Alice and Bob (in the ideal lossless case). We consider the standard situation in which Alice and Bob implement the optimal measurements to violate the CHSH inequality, given a singlet is shared, while the key is generated from one of these measurements, say $x = 0$. Therefore, Eve's goal is to guess the output of this measurement on Alice's side.

The correlations (23) can be conveniently arranged in a table as follows

$$\mathbf{p}^m = \left[\begin{array}{cc|cc} \eta_1 s & \eta_1 t & \eta_1 s & \eta_1 t \\ \eta_1 t & \eta_1 s & \eta_1 t & \eta_1 s \\ \frac{1-\eta_1}{2} & \frac{1-\eta_1}{2} & \frac{1-\eta_1}{2} & \frac{1-\eta_1}{2} \\ \hline \eta_1 s & \eta_1 t & \eta_1 t & \eta_1 s \\ \eta_1 t & \eta_1 s & \eta_1 s & \eta_1 t \\ \frac{1-\eta_1}{2} & \frac{1-\eta_1}{2} & \frac{1-\eta_1}{2} & \frac{1-\eta_1}{2} \end{array} \right], \quad (24)$$

where within each of the four blocks the columns are labelled by the two possible conclusive outputs of Bob, and the rows by the three outputs of Alice that include the non-detected outcome. The four blocks above correspond then to the four combinations of measurement settings $x, y = \{0, 1\}$, where $s = (1 + \cos(\pi/4))/4$ and $t = (1 - \cos(\pi/4))/4$. Whenever the local efficiency is unity, $\eta_1 = 1$, the correlations (24) violate maximally the CHSH inequality and are referred to as the 'Tsirelson correlations'.

It can be verified that the correlations (24) are local whenever $\eta_1 \leq 1/\sqrt{2}$. On the other hand, when using them to evaluate the bound (20) for any of Alice's

measurement, say $x = 0$, one obtains $I_E(S_{cc}, \mu) < 1$ whenever $\eta_1 > 1/\sqrt{2}$. The result is intuitively satisfactory: if the initial correlations are non-local, there is some uncertainty left for Eve about Alice's outcome after discarding the non-conclusive events. Unfortunately, this conclusion, and therefore the bound (20) used to derive it, is not universally valid, as proven by the following attack of Eve, whereby she has perfect knowledge of Alice's outcome for some values of η_1 larger than $1/\sqrt{2}$.

Eve prepares a mixture of the following three distributions:

$$\mathbf{p}_1 = \left[\begin{array}{cc|cc} s & t & s & t \\ t & s & t & s \\ 0 & 0 & 0 & 0 \\ \hline ps & pt & pt & ps \\ pt & ps & ps & pt \\ \frac{1}{2}(1-p) & \frac{1}{2}(1-p) & \frac{1}{2}(1-p) & \frac{1}{2}(1-p) \end{array} \right] \quad (25)$$

with $p = \sqrt{2} - 1 \approx 0.41$, which is local and, hence, can be further decomposed in terms of deterministic strategies; and

$$\mathbf{p}_2 = \left[\begin{array}{cc|cc} s & t & s & t \\ 0 & 0 & 0 & 0 \\ t & s & t & s \\ \hline s & t & t & s \\ t & s & s & t \\ 0 & 0 & 0 & 0 \end{array} \right], \quad \mathbf{p}_3 = \left[\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ t & s & t & s \\ s & t & s & t \\ \hline s & t & t & s \\ t & s & s & t \\ 0 & 0 & 0 & 0 \end{array} \right]. \quad (26)$$

The correlations (26) constitute ideal Tsirelson correlations (Eq. (24) with $\eta_1 = 1$ and re-labelled outcomes for Alice) and, therefore, are as non-local as the quantum mechanics allows. The important fact to notice is that for all \mathbf{p}_1 , \mathbf{p}_2 and \mathbf{p}_3 , if the no-click events are discarded, Eve has perfect knowledge on Alice's outcomes for $x = 0$, as can be seen by inspection from the tables.

We consider the following mixture

$$\mathbf{p}^\lambda = \lambda \mathbf{p}_1 + (1 - \lambda) \frac{1}{2} (\mathbf{p}_2 + \mathbf{p}_3) \quad (27)$$

and require the local efficiency to be outcome-independent. In particular, in order to reproduce the correlations (24), we solve

$$\eta_1 = \lambda + (1 - \lambda) \frac{1}{2} = \lambda p + (1 - \lambda) \quad (28)$$

for λ , so that $\mathbf{p}^\lambda = \mathbf{p}^m$. As a result, for $\lambda = \frac{1}{3-2p} = \frac{5+2\sqrt{2}}{17}$ we obtain an attack for which the correlations (24) are recovered with local efficiency:

$$\eta_1 = \frac{11 + \sqrt{2}}{17} \approx 0.73 \quad \left(> 1/\sqrt{2} \approx 0.707 \right). \quad (29)$$

As, once the non-conclusive events are discarded, Eve can then predict with certainty Alice's outcome for the setting $x = 0$, the above attack invalidates the upper bound (20) that predicts this to be impossible

for any $\eta_l > 1/\sqrt{2} \approx 0.707$. Although the bound (20) cannot thus hold in complete generality for situations including losses (as already speculated in Ref. [41]), it still remains to be proven whether Eq. (20) can be considered to be valid for the specific correlations arising in the protocol of Ref. [36].

D Heralded states produced by the SH and CH schemes

In Fig. 5 we depict once more the SH scheme—see its implementation in Fig. 3(a)—while separating explicitly the photonic modes involved, i.e. distinct modes originating from the labs of Alice and Bob (A and B) distinguished also by their polarisations (H and V), as well as the auxiliary modes (labelled as primed "'") that effectively are the ones to reach the heralding station, and are measured to obtain the heralding signal c . A protocol round is then accepted within the SH (and also CH, see below) scheme only if the click pattern $c = 0110 =: \odot$ is observed with only the two middle detectors in Fig. 5 clicking.

Within the SH scheme Alice uses the SPDC process to produce a pair of entangled photons in modes $A_{H/V}$ and $A'_{H/V}$ described by the state (12), ρ_{SPDC} . Bob employs on-demand sources in order to simultaneously prepare single photons (SPs) in modes B_H and B_V , each described by the state (16), σ_{SP} , see Fig. 5. Inspecting the expressions (12) and (16), the SH scheme ideally works at first order in \bar{p} and zeroth order in p , respectively, with higher orders being negligible due to $\bar{p} \lesssim 10^{-2}$ [23, 24] and $p \lesssim 10^{-4}$ [32]. For completeness, however, we perform the analysis up to second order in both p and \bar{p} by considering the initial (unnormalised and uncorrelated) state of Alice and Bob—i.e. the overall one present initially in the modes $A_{H/V}$, $A'_{H/V}$ and $B_{H/V}$ in Fig. 5—to read:

$$\begin{aligned} \rho_{\text{AB}}^{(\text{SH})} = & |0^{\text{AA}'}, 1_H^{\text{B}} 1_V^{\text{B}}\rangle\langle\ldots| + p |0^{\text{AA}'}, 1_H^{\text{B}} 2_V^{\text{B}}\rangle\langle\ldots| + \\ & p |0^{\text{AA}'}, 2_H^{\text{B}} 1_V^{\text{B}}\rangle\langle\ldots| + p^2 |0^{\text{AA}'}, 2_H^{\text{B}} 2_V^{\text{B}}\rangle\langle\ldots| + \\ & p^2 |0^{\text{AA}'}, 1_H^{\text{B}} 3_V^{\text{B}}\rangle\langle\ldots| + p^2 |0^{\text{AA}'}, 3_H^{\text{B}} 1_V^{\text{B}}\rangle\langle\ldots| + \\ & \bar{p} |\Psi_1^{\text{AA}'}, 1_H^{\text{B}} 1_V^{\text{B}}\rangle\langle\ldots| + \\ & p\bar{p} |\Psi_1^{\text{AA}'}, 1_H^{\text{B}} 2_V^{\text{B}}\rangle\langle\ldots| + p\bar{p} |\Psi_1^{\text{AA}'}, 2_H^{\text{B}} 1_V^{\text{B}}\rangle\langle\ldots| + \\ & \frac{3}{4} p^2 |\Psi_2^{\text{AA}'}, 1_H^{\text{B}} 1_V^{\text{B}}\rangle\langle\ldots| + O(p^i \bar{p}^j)_{i+j=3} \end{aligned} \quad (30)$$

with higher-order terms yielding negligible contributions, which nonetheless must be later accounted for (see App. F) when assuring the security of the DIQKD protocol.

Inspecting Eq. (30), it is the seventh term occurring at \bar{p} -order which is the desired one, containing an entangled pair $|\Psi_1\rangle$ in modes $A_{H/V}$ and $A'_{H/V}$ and single photons in both modes $B_{H/V}$. All other terms are spurious: the first six are associated with the vacuum production rounds of the SPDC source

held by Alice; the eighth and ninth correspond to cases in which the SPDC process succeeds but one of the SPs emits two photons instead; while the last term appears due to double-pair production of the SPDC. In order to compute the state $\rho_{\text{AB}|c}^{(\text{SH})}$ marked in Fig. 5, we propagate the initial state (30) “term by term” through the relevant parts of the circuit and account for the photon-detection measurement in modes $A'_{H/V}$ and $B'_{H/V}$, while assuming the detectors to be binary (on/off), i.e. clicking with efficiency η_h , without distinguishing the exact photon number.

Although we omit here the explicit expression for $\rho_{\text{AB}|c}^{(\text{SH})}$ that we obtain for $c = \odot$ (i.e. when only two out of the four relevant detectors in Fig. 5 click), we note that the leading order of $\rho_{\text{AB}|\odot}^{(\text{SH})}$ stated in Eq. (5) of the main text is the result of the desired contribution—the seventh term in Eq. (30). Crucially, contributions of all the other terms in Eq. (30) are suppressed due to $p, \bar{p} \ll 1$. Moreover, the impact of finite detection efficiency, $\eta_h < 1$, can be assumed to affect only the probability of successful heralding, i.e. $P(c = \odot)$ that corresponds to the norm of $\rho_{\text{AB}|\odot}^{(\text{SH})}$, because we ensure that $T \approx 1$ within the SH scheme. As a result, the SPs produced by Bob hardly enter the modes $B'_{H/V}$ in Fig. 5 or, in other words, leave the lab of Bob in Fig. 3(a).

Importantly, we use the full expression for $\rho_{\text{AB}|\odot}^{(\text{SH})}$ incorporating all the contributions of Eq. (30) to compute the resulting correlations shared by Alice and Bob after they measure photons in modes $A_{H/V}$ and $B_{H/V}$ in Fig. 5, respectively, i.e.:

$$P^{(\text{SH})} \left(a, b \left| \begin{array}{l} x = \{\phi_A, \theta_A\}, y = \{\phi_B, \theta_B\}, t, \eta_d, c = \odot \\ \eta_h, \eta_t, T \approx 1, p \approx 0, \bar{p} \approx 0 \end{array} \right. \right), \quad (31)$$

which similarly to the initial state (30) is valid up to $O(p^i \bar{p}^j)_{i+j=3}$. The form of the joint probability distribution (31) depends strongly on the measurement settings controlled by the angles (ϕ, θ) of polarization dual-rail qubits [76] detected by Alice and Bob, the efficiency η_d of the binary detectors they employ, as well as the t -parameter controlling the asymmetry of the heralding BSM (see Fig. 5) and, hence, the partial entanglement of the target state $|\psi_{\text{AB}}^t\rangle$ in Eq. (5). Nonetheless, we also list in the second row in Eq. (31) all the other parameters that the shared correlations formally depend on due to higher-order terms taken into account within the initial state (30).

However, in practice—as verified also by our numerical analysis—the dependence on the transmission loss parameter, η_t , as well as the efficiency of heralding detectors, η_h , can be completely disregarded as they enter Eq. (31) at higher order in p and $1 - T$, respectively. Nonetheless, let us emphasise that to compute both the critical local efficiencies, η_l^* , stated in Table 1 and the DIQKD key rates presented in Fig. 4, we use the full expression for the joint prob-

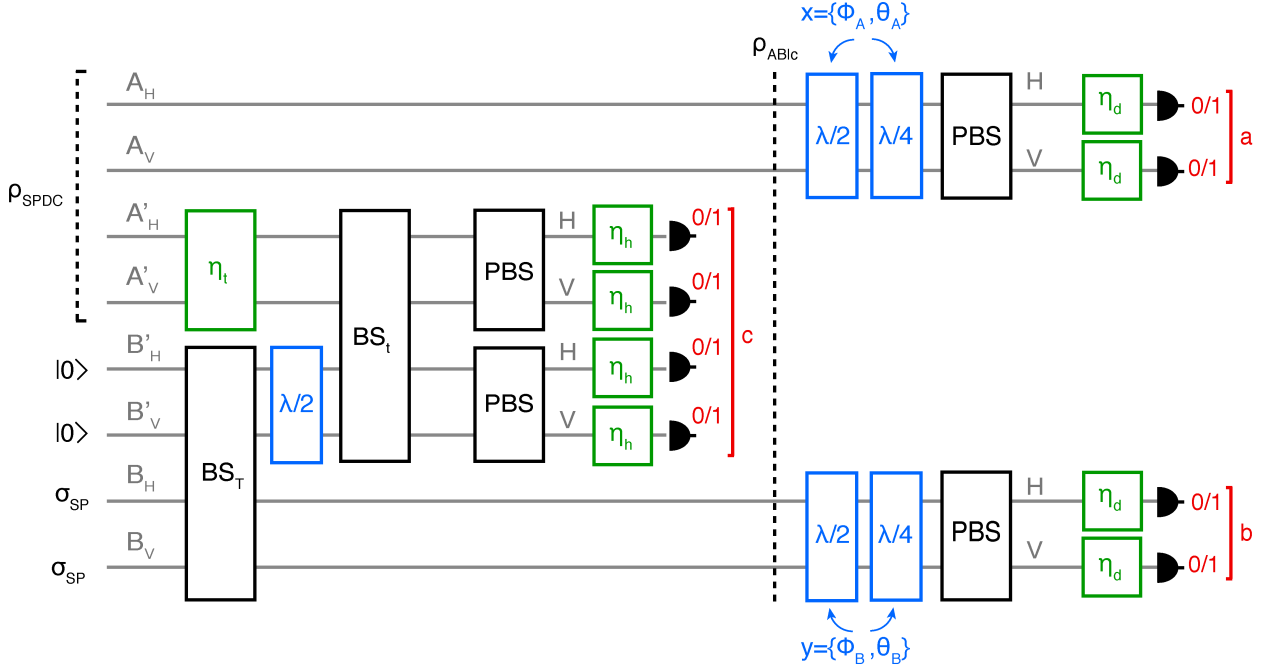


Figure 5: **SH scheme of Fig. 3(a) with all the photonic modes separated.** Alice employs a SPDC source to prepare entangled photon pairs in modes $A_{H/V}$ and $A'_{H/V}$ described by the state ρ_{SPDC} in Eq. (12). Bob uses two SP sources instead to simultaneously prepare single photons in modes $B_{H/V}$, each described by the state σ_{SP} in Eq. (16). The whole SH scheme corresponds to a linear-optics circuit involving beamsplitters (BSs), half- and quarter-wave plates ($\frac{\lambda}{4}$ and $\frac{\lambda}{4}$), polarising beamsplitters (PBSs), and binary detectors yielding "0" (for no photons) or "1" (when one or more photons are detected). The finite efficiency of heralding detectors, as well as ones held by Alice and Bob, is accounted for by loss parameters η_h and η_d , respectively, which similarly to the transmission loss, η_t , correspond to a BS-transformation with the vacuum state impinging the empty input port. In our analysis we consider the overall initial state $\rho_{\text{AB}}^{(\text{SH})}$ to be adequately described by its lowest-order expansion (30). We propagate it then through the circuit in order to compute the resulting state shared by Alice and Bob conditioned on successful heralding outcome, i.e. $\rho_{\text{AB}|c}^{(\text{SH})}$ with $c = 0110 =: \checkmark$ when only the middle two of the heralding detectors click. $\rho_{\text{AB}|\checkmark}$ is then the state spanning modes $A_{H/V}$ and $B_{H/V}$ that Alice and Bob perform dual-rail polarisation qubit measurements on, whose settings are completely parametrised by the angles $x = \{\phi_A, \theta_A\}$ and $y = \{\phi_B, \theta_B\}$ [76]. Finally, the outcomes a and b correspond to the four possible click patterns observed by Alice and Bob, respectively.

ability (31). In particular, we set the efficiency of the heralding detectors to be equal to the ones of Alice and Bob, i.e. $\eta_h = \eta_d =: \eta_l$, which in practice affects then only the key rate with $P(c = \checkmark) \propto \eta_l^2$ in Eq. (8). Moreover, in order to determine the highest key rates K in Eq. (8) that yield the lowest critical local efficiency, $\eta_l^* = \eta_d^*$, we also fine-tune the source parameters $\{\bar{p}, p, T\}$, whose orders of magnitude we importantly constrain to $\bar{p} \approx 10^{-2}$, $p \approx 10^{-4}$ and $(1 - T) \approx 10^{-3}$ for the lowest-order expansion analysis to always be valid.

For the CH scheme depicted Fig. 3(b), we follow exactly the same analysis as stated above for the SH scheme. The CH scheme can be presented as a similar linear optics circuit, where now the A-modes constitute just a copy (mirror image) of the B-modes drawn in Fig. 5. Within the CH scheme both Alice and Bob possess two on-demand SP sources. The only difference—due to the heralding station in Fig. 3(b) being held outside of the labs—are the transmission losses, η_t , that must now be accounted for not only

in the $A'_{H/V}$ (see Fig. 5) but also in the $B'_{H/V}$ modes.

However, for the CH scheme the initial state prepared by Alice and Bob (this time using only the four modes $A_{H/V}$ and $B_{H/V}$ in Fig. 5 with others containing vacuum) no longer contains spurious vacuum contributions, due to the SPDC process being absent, i.e.:

$$\begin{aligned} \rho_{\text{AB}}^{(\text{CH})} = & |1_H^A 1_V^A, 1_H^B 1_V^B\rangle\langle\ldots| + p |1_H^A 1_V^A, 1_H^B 2_V^B\rangle\langle\ldots| + \\ & p |1_H^A 1_V^A, 2_H^B 1_V^B\rangle\langle\ldots| + p |1_H^A 2_V^A, 1_H^B 1_V^B\rangle\langle\ldots| + \\ & p |2_H^A 1_V^A, 1_H^B 1_V^B\rangle\langle\ldots| + O(p^2), \end{aligned} \quad (32)$$

where, in contrast to Eq. (32), the ideal contribution occurs at zeroth order in p , that is, when each of the four SPs produces a single photon. Still, similarly to the SH scheme, we include higher-order contributions (now, at first order in p) in our analysis.

In particular, we compute the corresponding state $\rho_{\text{AB}|\checkmark}^{(\text{CH})}$ conditioned on successful heralding, whose main contribution comes from the zeroth-order in Eq. (32) stated in Eq. (6) of the main text. As in

Eq. (31), while keeping all the contributions of the initial state (32), we compute the shared correlations of Alice and Bob after they perform their measurements, i.e.:

$$P^{(\text{CH})}\left(a, b \left| \begin{array}{l} x = \{\phi_A, \theta_A\}, y = \{\phi_B, \theta_B\}, t, \eta_d, c = \bigcirc \\ \tilde{\eta}_t = \eta_h \eta_t, T \approx 0, p \approx 0 \end{array} \right. \right), \quad (33)$$

where in contrast to Eq. (31) the efficiency of the heralding detectors η_h —appearing in Eq. (33) again only due to higher-order terms in Eq. (32)—can be interpreted as just another source of effective transmission loss, $\tilde{\eta}_t$. As a result, in order for comparison of the key rates in Fig. 4 between the SH and CH schemes to be fair, we rescale $\eta_t \rightarrow \eta_t \eta_h$ in case of the latter to account for the heralding detectors to have the same efficiency as the ones held by Alice and Bob (i.e., $\eta_h = \eta_d = \eta_l$ in Fig. 5). Otherwise, we perform exactly the same analysis for the joint distribution (33) as for Eq. (31), in order to determine the maximal key rate, K in Eq. (4), and critical local efficiencies, η_l^* in Table 1, where we ensure now that $T \approx 10^{-3}$ and $p \lesssim 10^{-3}$ throughout the numerical optimisation, so that our perturbative approach (in photon number) assumed by Eq. (32) always holds.

Finally, let us note that within both the SH and CH schemes we may naturally account for the finite efficiency of the on-demand sources employed [25], which produce the SPs in the state (16), i.e. σ_{SP} marked in Fig. 5 for the SH scheme. Inspecting Fig. 5 and, in particular, modes $B_{H/V}$ —and similarly for the $A_{H/V}$ modes in case of the CH scheme, in which they are equivalent—it becomes clear that one may propagate beam-splitters responsible for the finite detection, η_d , all the way through the circuit onto the initial state without altering the scheme on the whole. Hence, given that each SP-source works with η_s -efficiency, all our analysis applies with now simply the overall local efficiency reading $\eta_l = \eta_s \eta_d$, so that it accounts for the finite efficiency of both the sources and detectors contained within the lab of Alice or Bob, or both (as summarised in the main text while including also finite transmission between these components, η_t).

E Guessing probability

The min-entropy term $-\log_2 G_{\mathbf{p}}(x^*)$ in Eq. (7) of the main text is expressed with help of the *device-independent guessing probability*, i.e. the average probability that the eavesdropper Eve correctly guesses the output of Alice using an optimal strategy: [77]

$$G_{\mathbf{p}}(x^*) := \max_{\{\mathbf{p}^e\}} \sum_e P(e) P(a = e | x^*, e) \quad (34)$$

s.t. $\sum_e \mathbf{p}^e = \mathbf{p}$ and $\forall e : \mathbf{p}^e \in \tilde{Q}.$

Here, $P(e)$ denotes the probability that Eve observes the outcome e , while $P(a = e | x^*, e)$ effectively repre-

sents the probability that Alice obtains an outcome a coinciding with e , given to be the one observed by Eve.

Any strategy of Eve in Eq. (34) can be seen as a measurement that she performs on her system, which then produces a decomposition (a collection) of unnormalized behaviours $\{\mathbf{p}^e\}$ distributed between Alice and Bob. The guessing probability (34) is then obtained by maximising the success of Eve's strategy over all such possible decompositions that, however, must reproduce on average the behaviour \mathbf{p} observed by Alice and Bob and be compatible with quantum mechanics (see the second line of Eq. (34)). Formally, each of them must belong to the set of unnormalised behaviours \tilde{Q} which stem from the Born's rule when valid quantum measurements act on an unnormalized, yet unspecified, quantum state. Thus, to enforce the *quantumness* of Eve's strategy, the second constraint in Eq. (34) demands that all \mathbf{p}^e belong to \tilde{Q} .

Imposing membership in \tilde{Q} is difficult since a precise characterization of \tilde{Q} is unknown. However, semi-definite programming (SDP) relaxations similar to the ones presented by Navascués et al. [78] can be introduced to bound $G_{\mathbf{p}}(x^*)$ from above [77]. One defines a convergent hierarchy of convex sets that have a precise characterization and obey $\tilde{Q}_1 \supseteq \tilde{Q}_2 \supseteq \dots \supseteq \tilde{Q}$. This hierarchy approximates the quantum set \tilde{Q} from outside, so that any optimisation over the quantum set can be relaxed (to some order k) by replacing \tilde{Q} in Eq. (34) with \tilde{Q}_k . Hence, the program presented in Eq. (34) becomes an SDP when relaxations of the set \tilde{Q} are employed—in our work we mostly consider relaxations to the order $1 + AB$, i.e. an intermediary order between first and second orders.

Finally, let us note that from the dual formulation [79] of the SDP program employed, we are also always able to retrieve the Bell inequality that is optimal for bounding the degree of predictability that a quantum eavesdropper may have about the string of Alice's outcomes [77].

F Dealing with higher-order multi-photon contributions

In order to deal with quantum states produced by SPDC and single-photon sources (presented in App. D), one typically truncates the global state produced by all sources in the setup up to a certain order n [36, 41, 42]. Since any setup we consider is powered by SPDC sources parameterized by \bar{p} and single-photon sources parametrized by p , a truncation to the order, e.g. $n = 2$ of the global state—which is the tensor product of the states of each source—would keep all terms up to order $O(p^2)$, $O(p\bar{p})$ and $O(\bar{p}^2)$.

Nevertheless, this perturbative approximation may yield misleading conclusions about the nonlocal char-

acter of the observed correlations and compromise DIQKD security for a given setup. In fact, one has to guarantee that contributions not considered in the truncation will not contradict the conclusions about the nonlocal character of the behaviour in question.

To avoid this problem, we develop here a method based on SDP techniques where all high-order contributions ($> n$) that are not taken into account are fully controlled by Eve, to her benefit. This may seem too conservative, but the method turns out to be efficient and not overly pessimistic, since the contribution of high-order terms becomes irrelevant for sufficiently low values of p and \bar{p} .

The key idea is to conceive higher-order contributions as producing an unknown and uncharacterized quantum behaviour \mathbf{p}_Q prepared by Eve for Alice and Bob. If $\mathbf{p}_n^{\text{est}}$ denotes the estimation of the behaviour of Alice and Bob constructed to the order n (e.g. one derived basing on states (30) or (32) for SH and CH-schemes, respectively), then the first step of the method is to write the observed behaviour \mathbf{p} as a convex decomposition: $\mathbf{p} = (1 - \epsilon_n)\mathbf{p}_n^{\text{est}} + \epsilon_n\mathbf{p}_Q$.

At the quantum level, the total state being shared, given a collection of sources producing a perturbative state such as (12), may be written as a convex mixture $p(n)\rho_n + p(\bar{n})\rho_{\bar{n}}$, where ρ_n is the truncated state according to the estimation made at some order n . $\rho_{\bar{n}}$ is thus the remaining “tail” of high-order contributions, and $p(\bar{n}) = 1 - p(n)$. Moving to the level of probability distributions, linearity of Born’s rule with respect to ρ implies that the elements of the observed behaviour \mathbf{p} conditioned on the outcome c employed in the heralding stage (see App. D) may be decomposed in a similar fashion, i.e.:

$$P(a, b|c) = p(n|c)P(a, b|c, n) + p(\bar{n}|c)P(a, b|c, \bar{n}). \quad (35)$$

The probabilities $P(a, b|c, n)$ above are then nothing but the elements of the estimated behaviour $\mathbf{p}_n^{\text{est}}$ computed up to the n th order.

We rewrite $p(n|c)$ employing the Bayes rule:

$$p(n|c) = \frac{p(c|n)p(n)}{p(c)}. \quad (36)$$

The numerator in Eq. (36) is known, as $p(c|n)$ is merely the probability of observing the heralding outcome c while assuming the n th order truncation at the level of the sources. The denominator, however, is unknown and corresponds to the probability of observing the outcome c , without assuming any truncation.

Still, it is possible to set an upper bound on $p(c)$:

$$\begin{aligned} p(c) &= \sum_{\vec{k}=\vec{0}}^{\infty} p(\vec{k})p(c|\vec{k}) \\ &\leq p_{\vec{K}_n}(c) := \sum_{\vec{k}=\vec{0}}^{\vec{K}_n} p(\vec{k})p(c|\vec{k}) + \sum_{\vec{k} > \vec{K}_n} p(\vec{k}), \end{aligned} \quad (37)$$

where the vector of variables $\vec{k} = (k_1, k_2, \dots, k_s)$ describes the possible number of photons produced by each of the s sources. In particular, $p(\vec{k})$ gives the distribution for each of the possible combinations of photons (or photon pairs) occurring, when produced by the sources. Vector \vec{K}_n contains the numbers of photons that each source can maximally produce, given a particular order n of the truncation.

Bounding Eq. (36) with help of Eq. (37), one gets the desired upper bound on $\epsilon_n = 1 - p(n|c)$, i.e.,

$$\epsilon_n \leq \epsilon_n^\uparrow := 1 - \frac{p(c|n)p(n)}{p_{\vec{K}_n}(c)}, \quad (38)$$

which can be importantly computed for a given optical scheme and the order n assumed. Consistently, ϵ_n^\uparrow (and, hence, ϵ_n) goes to zero as the order n increases, so that $\mathbf{p}_n^{\text{est}}$ converges to \mathbf{p} in the limit $n \rightarrow \infty$.

In an analogous way to Eq. (34), we define the *device-independent guessing probability to the order n* as:

$$\begin{aligned} G_{\mathbf{p}_n^{\text{est}}}(x^*, \epsilon) &:= \max_{\{\mathbf{p}^e\}} \sum_e P(e, a = e|x^*) \\ \text{s.t. } \sum_e \mathbf{p}^e &= (1 - \epsilon)\mathbf{p}_n^{\text{est}} + \epsilon\mathbf{p}_Q, \\ \mathbf{p}_Q &\in Q \text{ and } \forall e : \mathbf{p}^e \in \tilde{Q}, \end{aligned} \quad (39)$$

where $(\tilde{Q})Q$ denotes the set of (un)normalized quantum behaviours. The crucial difference between Eqs. (34) and (39) is that Eve is now *not* obliged to reproduce exactly the behaviour \mathbf{p} with her collection of unnormalised behaviours $\{\mathbf{p}^e\}$. Instead, she possesses a supplementary quantum behaviour \mathbf{p}_Q that she can tailor, so that it is easier for her to reproduce the behaviour $\mathbf{p}_n^{\text{est}}$ for a given *fixed* value of ϵ and, hence, better guess the outcome of Alice’s box.

Now, the following inequalities must hold:

$$G_{\mathbf{p}_n^{\text{est}}}(x^*) \leq G_{\mathbf{p}_n^{\text{est}}}(x^*, \epsilon_n) \leq G_{\mathbf{p}_n^{\text{est}}}(x^*, \epsilon_n^\uparrow), \quad (40)$$

where the first one is guaranteed to be saturated whenever it is optimal to set $\mathbf{p}_Q = \mathbf{p}_n^{\text{est}}$ in Eq. (39) (i.e. the truncation plays no role), while the second one whenever the bound (38) is tight. As a result, we may always upper-bound Eve’s optimal guessing probability by $G_{\mathbf{p}_n^{\text{est}}}(x^*, \epsilon_n^\uparrow)$, and by doing so we can only underestimate the attainable key rate of the DIQKD protocol—see Eq. (7) of the main text.

Let us stress that the method presented above is quite general, as it can be applied to any other uncharacterised imperfection parametrised by ϵ , such that its action arises as convex decomposition of the form $\mathbf{p} = (1 - \epsilon)\mathbf{p}_n^{\text{est}} + \epsilon\mathbf{p}_Q$. In particular, it allows to upper-bound the guessing probability for any type of noise that may be represented as a convex mixture at the level of a quantum state, given that the corresponding mixing probability can also be bound from above by a known $\epsilon^\uparrow < 1$.

G Noise robustness for nonlocality

We analyze the robustness to white noise of the estimated behaviours \mathbf{p}^{est} that our two schemes produce. We determine the maximal value w^* of white noise $\mathbf{1}_{\mathbf{p}}$ —a distribution in which all the outcomes are equally likely, independently of the measurement choices—which can be convexly added such that the behaviour $(1 - w)\mathbf{p}^{\text{est}} + w\mathbf{1}_{\mathbf{p}}$ remains nonlocal.

Membership of a probability distribution to the set of local behaviours [9] is an instance of a linear program [79]. Geometrically speaking, the set of local behaviours is a polytope in the space of probability distributions, whose extremal points correspond to particular deterministic strategies $\{\mathbf{D}_{\mu}\}_{\mu}$ that are sufficient to decompose any local behaviour. In fact, there is a finite number of such deterministic strategies, and the white noise tolerance of \mathbf{p}^{est} is given by the solution of the following linear program:

$$\begin{aligned} w^* &= \min_{\{q_{\mu}\}} w & (41) \\ \text{s.t. } (1 - w)\mathbf{p}^{\text{est}} + w\mathbf{1}_{\mathbf{p}} &= \sum_{\mu} q_{\mu}\mathbf{D}_{\mu}, \\ \sum_{\mu} q_{\mu} &= 1 \text{ and } \forall \mu : q_{\mu} \geq 0. \end{aligned}$$

The white-noise tolerance threshold, w^* , should be interpreted as deviations from the desired correlations at the level of probability distributions. This is the worst-case approach in which the experimental imperfections not accounted for in \mathbf{p}^{est} provide Alice and Bob with completely uncorrelated results. The fact that our schemes tolerate high amounts of white noise (see Table 1 of the main text) ensures that our results will not be strongly affected when introducing other sources of noise, not accounted for in the analysis.

References

- [1] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th IEEE Conference on Foundations of Computer Science*, 1998.
- [2] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98:230501, June 2007. DOI: [10.1103/PhysRevLett.98.230501](https://doi.org/10.1103/PhysRevLett.98.230501).
- [3] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New J. Phys.*, 11(4):045021, April 2009. DOI: [10.1088/1367-2630/11/4/045021](https://doi.org/10.1088/1367-2630/11/4/045021).
- [4] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key

- distribution with causally independent measurement devices. *Nat. Commun.*, 2:238–, March 2011. DOI: [10.1038/ncomms1244](https://doi.org/10.1038/ncomms1244).
- [5] S. Pironio, Ll. Masanes, A. Leverrier, and A. Acín. Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model. *Phys. Rev. X*, 3:031007, August 2013. DOI: [10.1103/PhysRevX.3.031007](https://doi.org/10.1103/PhysRevX.3.031007).
- [6] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, September 2014. DOI: [10.1103/PhysRevLett.113.140501](https://doi.org/10.1103/PhysRevLett.113.140501).
- [7] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *SIAM J. Comput.*, 48(1):181–225, 2019. DOI: [10.1137/18M1174726](https://doi.org/10.1137/18M1174726).
- [8] John Bell. On the Einstein-Podolsky-Rosen Paradox. *Physics*, 1:195–200, 1964. DOI: [10.1103/physicsphysiquefizika.1.195](https://doi.org/10.1103/physicsphysiquefizika.1.195).
- [9] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, April 2014. DOI: [10.1103/RevModPhys.86.419](https://doi.org/10.1103/RevModPhys.86.419).
- [10] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, October 1970. DOI: [10.1103/PhysRevD.2.1418](https://doi.org/10.1103/PhysRevD.2.1418).
- [11] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Valerio Scarani, Vadim Makarov, and Christian Kurtsiefer. Experimentally Faking the Violation of Bell’s Inequalities. *Phys. Rev. Lett.*, 107:170404, October 2011. DOI: [10.1103/PhysRevLett.107.170404](https://doi.org/10.1103/PhysRevLett.107.170404).
- [12] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, October 1969. DOI: [10.1103/PhysRevLett.23.880](https://doi.org/10.1103/PhysRevLett.23.880).
- [13] Philippe H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A*, 47:R747–R750, February 1993. DOI: [10.1103/PhysRevA.47.R747](https://doi.org/10.1103/PhysRevA.47.R747).
- [14] M. A. Rowe, D. Kielpinski, V. Meyer, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell’s inequality with efficient detection. *Nature*, 409, February 2001. DOI: [10.1038/35057215](https://doi.org/10.1038/35057215).
- [15] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe. Bell inequality violation with two remote atomic qubits. *Phys. Rev. Lett.*, 100:150404, April 2008. DOI: [10.1103/PhysRevLett.100.150404](https://doi.org/10.1103/PhysRevLett.100.150404).
- [16] Julian Hofmann, Michael Krug, Norbert Ortégel, Lea Gérard, Markus Weber, Wenjamin Rosenfeld, and Harald Weinfurter. Heralded entanglement between widely separated atoms. *Science*, 337(6090):72–75, 2012. DOI: [10.1126/science.1221856](https://doi.org/10.1126/science.1221856).

- [17] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682–686, October 2015. DOI: [10.1038/nature15759](https://doi.org/10.1038/nature15759).
- [18] Alejandro Máttar, Jonatan Bohr Brask, and Antonio Acín. Device-independent quantum key distribution with spin-coupled cavities. *Phys. Rev. A*, 88:062319, December 2013. DOI: [10.1103/PhysRevA.88.062319](https://doi.org/10.1103/PhysRevA.88.062319).
- [19] Nicolas Brunner, Andrew B Young, Chengyong Hu, and John G Rarity. Proposal for a loophole-free Bell test based on spin-photon interactions in cavities. *New J. Phys.*, 15(10):105006, 2013. DOI: [10.1088/1367-2630/15/10/105006](https://doi.org/10.1088/1367-2630/15/10/105006).
- [20] N. Sangouard, J.-D. Bancal, N. Gisin, W. Rosenfeld, P. Sekatski, M. Weber, and H. Weinfurter. Loophole-free Bell test with one atom and less than one photon on average. *Phys. Rev. A*, 84:052122, November 2011. DOI: [10.1103/PhysRevA.84.052122](https://doi.org/10.1103/PhysRevA.84.052122).
- [21] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jorn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, Rupert Ursin, and Anton Zeilinger. Bell violation using entangled photons without the fair-sampling assumption. *Nature*, 497:227–230, September 2013. DOI: [10.1038/nature12012](https://doi.org/10.1038/nature12012).
- [22] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Phys. Rev. Lett.*, 111:130406, September 2013. DOI: [10.1103/PhysRevLett.111.130406](https://doi.org/10.1103/PhysRevLett.111.130406).
- [23] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons. *Phys. Rev. Lett.*, 115:250401, December 2015. DOI: [10.1103/PhysRevLett.115.250401](https://doi.org/10.1103/PhysRevLett.115.250401).
- [24] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong Loophole-Free Test of Local Realism. *Phys. Rev. Lett.*, 115:250402, December 2015. DOI: [10.1103/PhysRevLett.115.250402](https://doi.org/10.1103/PhysRevLett.115.250402).
- [25] Igor Aharonovich, Dirk Englund, and Milos Toth. Solid-state single-photon emitters. *Nat. Photonics*, 10(10):631–641, October 2016. ISSN 1749-4885. DOI: [10.1038/nphoton.2016.186](https://doi.org/10.1038/nphoton.2016.186).
- [26] Markus Müller, Samir Bounouar, Klaus D Jöns, M Glässl, and P Michler. On-demand generation of indistinguishable polarization-entangled photon pairs. *Nat. Photonics*, 8(3):224–228, March 2014. ISSN 1749-4885. DOI: [10.1038/nphoton.2013.377](https://doi.org/10.1038/nphoton.2013.377).
- [27] Julien Claudon, Joel Bleuse, Nitin Singh Malik, Maela Bazin, Perine Jaffrennou, Niels Gregersen, Christophe Sauvan, Philippe Lalanne, and Jean-Michel Gerard. A highly efficient single-photon source based on a quantum dot in a photonic nanowire. *Nat. Photonics*, 4(3):174–177, March 2010. ISSN 1749-4885. DOI: [10.1038/nphoton.2009.287](https://doi.org/10.1038/nphoton.2009.287).
- [28] Juan C Loredó, Nor A Zakaria, Niccolò Somaschi, Carlos Anton, Lorenzo De Santis, Valerian Giesz, Thomas Grange, Matthew A Broome, Olivier Gazzano, Guillaume Coppola, et al. Scalable performance in solid-state single-photon sources. *Optica*, 3(4):433–440, 2016. DOI: [10.1364/OPTICA.3.000433](https://doi.org/10.1364/OPTICA.3.000433).
- [29] Hui Wang, Z.-C. Duan, Y.-H. Li, Si Chen, J.-P. Li, Y.-M. He, M.-C. Chen, Yu He, X. Ding, Cheng-Zhi Peng, Christian Schneider, Martin Kamp, Sven Höfling, Chao-Yang Lu, and Jian-Wei Pan. Near-transform-limited single photons from an efficient solid-state quantum emitter. *Phys. Rev. Lett.*, 116:213601, May 2016. DOI: [10.1103/PhysRevLett.116.213601](https://doi.org/10.1103/PhysRevLett.116.213601).
- [30] Je-Hyung Kim, Tao Cai, Christopher J. K. Richardson, Richard P. Leavitt, and Edo Waks. Two-photon interference from a bright single-photon source at telecom wavelengths. *Optica*, 3(6):577–584, June 2016. DOI: [10.1364/OPTICA.3.000577](https://doi.org/10.1364/OPTICA.3.000577).
- [31] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredó, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, C. Gomez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaitre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart. Near-optimal single-photon

- sources in the solid state. *Nat. Photonics*, March 2016. DOI: [10.1038/nphoton.2016.23](https://doi.org/10.1038/nphoton.2016.23).
- [32] Xing Ding, Yu He, Z.-C. Duan, Niels Gregersen, M.-C. Chen, S. Unsleber, S. Maier, Christian Schneider, Martin Kamp, Sven Höfling, Chao-Yang Lu, and Jian-Wei Pan. On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Phys. Rev. Lett.*, 116:020401, January 2016. DOI: [10.1103/PhysRevLett.116.020401](https://doi.org/10.1103/PhysRevLett.116.020401).
- [33] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337–4341, December 1995. DOI: [10.1103/PhysRevLett.75.4337](https://doi.org/10.1103/PhysRevLett.75.4337).
- [34] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Tech. J.*, 28(4):656–715, 1949. DOI: [10.1002/j.1538-7305.1949.tb00928.x](https://doi.org/10.1002/j.1538-7305.1949.tb00928.x).
- [35] Alejandro Máttar and Antonio Acín. Implementations for device-independent quantum key distribution. *Phys. Scr.*, 91(4):043003, 2016. DOI: [10.1088/0031-8949/91/4/043003](https://doi.org/10.1088/0031-8949/91/4/043003).
- [36] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, August 2010. DOI: [10.1103/PhysRevLett.105.070501](https://doi.org/10.1103/PhysRevLett.105.070501).
- [37] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6(9):659–662, September 2010. ISSN 1745-2473, 1745-2481. DOI: [10.1038/nphys1734](https://doi.org/10.1038/nphys1734).
- [38] Marco Tomamichel and Esther Hänggi. The link between entropic uncertainty and nonlocality. *J. Phys. A: Math. Theor.*, 46(5):055301, January 2013. ISSN 1751-8121. DOI: [10.1088/1751-8113/46/5/055301](https://doi.org/10.1088/1751-8113/46/5/055301).
- [39] Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. Device-independent quantum key distribution with local bell test. *Phys. Rev. X*, 3:031006, July 2013. DOI: [10.1103/PhysRevX.3.031006](https://doi.org/10.1103/PhysRevX.3.031006).
- [40] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, August 2000. DOI: [10.1103/PhysRevLett.85.1330](https://doi.org/10.1103/PhysRevLett.85.1330).
- [41] Marcos Curty and Tobias Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84:010304, July 2011. DOI: [10.1103/PhysRevA.84.010304](https://doi.org/10.1103/PhysRevA.84.010304).
- [42] Evan Meyer-Scott, Marek Bula, Karol Bartkiewicz, Antonín Černoch, Jan Soubusta, Thomas Jennewein, and Karel Lemr. Entanglement-based linear-optical qubit amplifier. *Phys. Rev. A*, 88:012327, July 2013. DOI: [10.1103/PhysRevA.88.012327](https://doi.org/10.1103/PhysRevA.88.012327).
- [43] Kaushik P. Seshadreesan, Masahiro Takeoka, and Masahide Sasaki. Progress towards practical device-independent quantum key distribution with spontaneous parametric down-conversion sources, on-off photodetectors, and entanglement swapping. *Phys. Rev. A*, 93:042328, April 2016. DOI: [10.1103/PhysRevA.93.042328](https://doi.org/10.1103/PhysRevA.93.042328).
- [44] David Pitkanen, Xiongfeng Ma, Ricardo Wickert, Peter van Loock, and Norbert Lütkenhaus. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Phys. Rev. A*, 84:022325, August 2011. DOI: [10.1103/PhysRevA.84.022325](https://doi.org/10.1103/PhysRevA.84.022325).
- [45] Antonio Acín, Daniel Cavalcanti, Elsa Passaro, Stefano Pironio, and Paul Skrzypczyk. Necessary detection efficiencies for secure quantum key distribution and bound randomness. *Phys. Rev. A*, 93:012319, January 2016. DOI: [10.1103/PhysRevA.93.012319](https://doi.org/10.1103/PhysRevA.93.012319).
- [46] M. Arcari, I. Söllner, A. Javadi, S. Lindskov Hansen, S. Mahmoodian, J. Liu, H. Thyrrestrup, E. H. Lee, J. D. Song, S. Stobbe, and P. Lodahl. Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide. *Phys. Rev. Lett.*, 113:093603, August 2014. DOI: [10.1103/PhysRevLett.113.093603](https://doi.org/10.1103/PhysRevLett.113.093603).
- [47] Stephen Wein, Nikolai Lauk, Roohollah Ghobadi, and Christoph Simon. Feasibility of efficient room-temperature solid-state sources of indistinguishable single photons using ultrasmall mode volume cavities. *Phys. Rev. B*, 97:205418, May 2018. DOI: [10.1103/PhysRevB.97.205418](https://doi.org/10.1103/PhysRevB.97.205418).
- [48] Chris Gustin and Stephen Hughes. Influence of electron-phonon scattering for an on-demand quantum dot single-photon source using cavity-assisted adiabatic passage. *Phys. Rev. B*, 96:085305, August 2017. DOI: [10.1103/PhysRevB.96.085305](https://doi.org/10.1103/PhysRevB.96.085305).
- [49] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93% system efficiency. *Nat. Photonics*, 7(3):210–214, March 2013. ISSN 1749-4893. DOI: [10.1038/nphoton.2013.13](https://doi.org/10.1038/nphoton.2013.13).
- [50] Jun Zhang, Mark A. Itzler, Hugo Zbinden, and Jian-Wei Pan. Advances in InGaAs/InP single-photon detector systems for quantum communication. *Light Sci. Appl.*, 4:e286, 2015. ISSN 2047-7538. DOI: [10.1038/lsa.2015.59](https://doi.org/10.1038/lsa.2015.59).
- [51] Shigehito Miki, Masahiro Yabuno, Taro Yamashita, and Hirotaka Terai. Stable, high-performance operation of a fiber-coupled super-

- conducting nanowire avalanche photon detector. *Opt. Express*, 25(6):6796–6804, March 2017. ISSN 1094-4087. DOI: [10.1364/OE.25.006796](https://doi.org/10.1364/OE.25.006796).
- [52] Maria Moshkova, Alexander Divochiy, Pavel Morozov, Yury Vakhtomin, Andrey Antipov, Philipp Zolotov, Vitaly Seleznev, Marat Ahmetov, and Konstantin Smirnov. High-performance superconducting photon-number-resolving detectors with 86% system efficiency at telecom range. *J. Opt. Soc. Am. B, JOSAB*, 36(3):B20–B25, March 2019. DOI: [10.1364/JOSAB.36.000B20](https://doi.org/10.1364/JOSAB.36.000B20).
- [53] Lan Zhou, Yu-Bo Sheng, and Gui-Lu Long. Device-independent quantum secure direct communication against collective attacks. *Science Bulletin*, 65(1):12–20, 2020. ISSN 2095-9273. DOI: [10.1016/j.scib.2019.10.025](https://doi.org/10.1016/j.scib.2019.10.025).
- [54] Philippe Grangier, Juan Ariel Levenson, and Jean-Philippe Poizat. Quantum non-demolition measurements in optics. *Nature*, 396(6711):537–542, December 1998. ISSN 0028-0836. DOI: [10.1038/25059](https://doi.org/10.1038/25059).
- [55] B. C. Jacobs, T. B. Pittman, and J. D. Franson. Quantum relays and noise suppression using linear optics. *Phys. Rev. A*, 66:052307, November 2002. DOI: [10.1103/PhysRevA.66.052307](https://doi.org/10.1103/PhysRevA.66.052307).
- [56] Pieter Kok, Hwang Lee, and Jonathan P. Dowling. Single-photon quantum-nondemolition detectors constructed with linear optics and projective measurements. *Phys. Rev. A*, 66:063814, December 2002. DOI: [10.1103/PhysRevA.66.063814](https://doi.org/10.1103/PhysRevA.66.063814).
- [57] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: Entangling photons that never interacted. *Phys. Rev. Lett.*, 80:3891–3894, May 1998. DOI: [10.1103/PhysRevLett.80.3891](https://doi.org/10.1103/PhysRevLett.80.3891).
- [58] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. F. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell’s theorem. *Nature*, 464, April 2010. DOI: [10.1038/nature09008](https://doi.org/10.1038/nature09008).
- [59] Mikołaj Lasota, Czesław Radzewicz, Konrad Banaszek, and Rob Thew. Linear optics schemes for entanglement distribution with realistic single-photon sources. *Phys. Rev. A*, 90:033836, September 2014. DOI: [10.1103/PhysRevA.90.033836](https://doi.org/10.1103/PhysRevA.90.033836).
- [60] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, September 2009. DOI: [10.1103/RevModPhys.81.1301](https://doi.org/10.1103/RevModPhys.81.1301).
- [61] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.*, 108:100402, March 2012. DOI: [10.1103/PhysRevLett.108.100402](https://doi.org/10.1103/PhysRevLett.108.100402).
- [62] Qiang Zhang, Xiuping Xie, Hiroki Takesue, Sae Woo Nam, Carsten Langrock, M. M. Fejer, and Yoshihisa Yamamoto. Correlated photon-pair generation in reverse-proton-exchange ppln waveguides with integrated mode demultiplexer at 10 ghz clock. *Opt. Express*, 15(16):10288–10293, August 2007. DOI: [10.1364/oe.15.010288](https://doi.org/10.1364/oe.15.010288).
- [63] Cezary Śliwa and Konrad Banaszek. Conditional preparation of maximal polarization entanglement. *Phys. Rev. A*, 67(3):030101, March 2003. DOI: [10.1103/PhysRevA.67.030101](https://doi.org/10.1103/PhysRevA.67.030101).
- [64] Stefanie Barz, Gunther Cronenberg, Anton Zeilinger, and Philip Walther. Heralded generation of entangled photon pairs. *Nat. Photonics*, 4(8):553–556, August 2010. ISSN 1749-4893. DOI: [10.1038/nphoton.2010.156](https://doi.org/10.1038/nphoton.2010.156).
- [65] Claudia Wagenknecht, Che-Ming Li, Andreas Reingruber, Xiao-Hui Bao, Alexander Goebel, Yu-Ao Chen, Qiang Zhang, Kai Chen, and Jian-Wei Pan. Experimental demonstration of a heralded entanglement source. *Nat. Photonics*, 4(8):549–552, August 2010. ISSN 1749-4893. DOI: [10.1038/nphoton.2010.123](https://doi.org/10.1038/nphoton.2010.123).
- [66] C. L. Salter, R. M. Stevenson, I. Farrer, C. A. Nicoll, D. A. Ritchie, and A. J. Shields. An entangled-light-emitting diode. *Nature*, 465(7298):594–597, June 2010. ISSN 1476-4687. DOI: [10.1038/nature09078](https://doi.org/10.1038/nature09078).
- [67] R. M. Stevenson, C. L. Salter, J. Nilsson, A. J. Bennett, M. B. Ward, I. Farrer, D. A. Ritchie, and A. J. Shields. Indistinguishable Entangled Photons Generated by a Light-Emitting Diode. *Phys. Rev. Lett.*, 108(4):040503, January 2012. DOI: [10.1103/PhysRevLett.108.040503](https://doi.org/10.1103/PhysRevLett.108.040503).
- [68] Rinaldo Trotta, Johannes S. Wildmann, Eugenio Zallo, Oliver G. Schmidt, and Armando Rastelli. Highly Entangled Photons from Hybrid Piezoelectric-Semiconductor Quantum Dot Devices. *Nano Lett.*, 14(6):3439–3444, June 2014. ISSN 1530-6984. DOI: [10.1021/nl500968k](https://doi.org/10.1021/nl500968k).
- [69] Le Phuc Thinh, Gonzalo de la Torre, Jean-Daniel Bancal, Stefano Pironio, and Valerio Scarani. Randomness in post-selected events. *New J. Phys.*, 18(3):035007, 2016. DOI: [10.1088/1367-2630/18/3/035007](https://doi.org/10.1088/1367-2630/18/3/035007).
- [70] Ernest Y.-Z. Tan, Charles C.-W. Lim, and Renato Renner. Advantage distillation for device-independent quantum key distribution. *Phys. Rev. Lett.*, 124(2):020502, January 2020. DOI: [10.1103/PhysRevLett.124.020502](https://doi.org/10.1103/PhysRevLett.124.020502).
- [71] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt.*

- Photonics*, 2019. DOI: [10.1364/aop.361502](https://doi.org/10.1364/aop.361502). URL <https://arxiv.org/abs/1906.01645>.
- [72] Víctor Zapatero and Marcos Curty. Long-distance device-independent quantum key distribution. *Sci. Rep.*, 9, 2019. ISSN 2045-2322. DOI: [10.1038/s41598-019-53803-0](https://doi.org/10.1038/s41598-019-53803-0).
 - [73] G. Murta, S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner. Towards a realization of device-independent quantum key distribution. *Quantum Sci. Technol.*, 4(3):035011, July 2019. DOI: [10.1088/2058-9565/ab2819](https://doi.org/10.1088/2058-9565/ab2819).
 - [74] Yoshiaki Tsujimoto, Chenglong You, Kentaro Wakui, Mikio Fujiwara, Kazuhiro Hayasaka, Shigehito Miki, Hirotaka Terai, Masahide Sasaki, Jonathan P Dowling, and Masahiro Takeoka. Heralded amplification of nonlocality via entanglement swapping. *New J. Phys.*, 22(2):023008, February 2020. DOI: [10.1088/1367-2630/ab61da](https://doi.org/10.1088/1367-2630/ab61da).
 - [75] Pieter Kok and Samuel L. Braunstein. Post-selected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61:042304, March 2000. DOI: [10.1103/PhysRevA.61.042304](https://doi.org/10.1103/PhysRevA.61.042304).
 - [76] Tim C. Ralph and Geoff J. Pryde. Chapter 4 - Optical Quantum Computation. In *Progress in Optics*, volume 54, pages 209–269. Elsevier, January 2010. DOI: [10.1016/S0079-6638\(10\)05409-0](https://doi.org/10.1016/S0079-6638(10)05409-0).
 - [77] O. Nieto-Silleras, S. Pironio, and J. Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.*, 16(1):013035, January 2014. DOI: [10.1088/1367-2630/16/1/013035](https://doi.org/10.1088/1367-2630/16/1/013035).
 - [78] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, January 2007. DOI: [10.1103/PhysRevLett.98.010401](https://doi.org/10.1103/PhysRevLett.98.010401).
 - [79] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, New York, NY, USA, 2004. ISBN 0521833787. DOI: [10.1017/cbo9780511804441](https://doi.org/10.1017/cbo9780511804441).